VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA

EKONOMICKÁ FAKULTA

KATEDRA MANAGEMENTU

Analýza informační strategie ve vybraném podniku

Analysis of Information Strategy in a Chosen Company

Studentka: Bc. Lucie Odehnalová

Vedoucí diplomové práce: Ing. David Nespěšný, MBA

Ostrava 2012

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra managementu

Zadání diplomové práce

Student: **Bc. Lucie Odehnalová**

Studijní program: N6208 Ekonomika a management

Studijní obor: 6208T037 Management

Téma: Analýza informační strategie ve vybraném podniku
Analysis of Information Strategy in a Chosen Company

Zásady pro vypracování:

1. Úvod
2. Teoretická východiska informační strategie
3. Charakteristika zemědělského podniku
4. Analýza současného stavu informační strategie v podniku
5. Návrhy a doporučení pro zdokonalení
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

SKLENÁK, Vilém et al. *Data, informace, znalosti a Internet.* Praha: C. H. Beck, 2001. ISBN 80-7179-409-0.
TRUNEČEK, Jan et al. *Management v informační společnosti.* Praha: VŠE, 2004. ISBN 80-7079-201-9.
VYMĚTAL, Jan et al. *Informační a znalostní management v praxi.* Praha: LexisNexis CZ, 2006. ISBN 80-86920-01-1.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. David Nespěšný, MBA**

Datum zadání: 25.11.2011
Datum odevzdání: 27.04.2012

VYSOKÁ ŠKOLA BÁŇSKO-TECHNICKÁ UNIVERZITA Ekonomická fakulta 1 OSTRAVA

Ing. Petra Horváthová, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Prohlášení

Místopřísežně prohlašuji, že jsem celou diplomovou práci včetně všech příloh vypracovala samostatně. K práci jsem použila literatury a pramenů uvedených v seznamu.

V Ostravě ....

Poděkování

Touto cestou bych ráda poděkovala svému vedoucímu diplomové práce panu Ing. Davidu Nespěšnému, MBA za pomoc při její tvorbě, za cenné rady a doporučení. Dále velké díky patří vedení firmy LUKROM, spol. s r.o., která mi umožnila přístup k informacím a následnému zpracování praktické části, zejména pak panu Ing. Janu Esterkovi za mimořádně pozitivní přístup a jeho čas. A v neposlední řadě bych chtěla poděkovat i zaměstnancům a jejich ochotě ke spolupráci.

OBSAH

1 ÚVOD

Diplomová práce je kombinací problematiky vytvořené z oblasti informační a manažerské. Zaobírá se aktuální situací informační společnosti, jejími negativními a pozitivními aspekty, informačními hrozbami a celou řadou důsledků, které ze současného vývoje plynou pro každý podnik. Ze širokého okruhu soudobých výzev se práce věnuje konkrétní otázce informační strategie, která je charakteristická svou komplexností a zasahuje napříč spektrem různých oblastí a směrů, což je typické také pro tuto práci.

Základním motivem k výběru tohoto tématu byla především jeho aktuálnost, důležitost ve vztahu jak k podnikům, tak i k běžným uživatelům, bezprostřední setkání téměř každého s danou problematikou a určitou dávkou podceňování jak hrozeb, tak i příležitostí,
a touto cestou tak poodkrýt alespoň část změn, které nemůžeme zastavit ani ignorovat, ale právě se adaptovat a těžit z jejich výhod a minimalizovat jejich nedostatky a rizika.

Vzhledem k turbulentnímu rozvoji technologií je nutné, aby se každá společnost přizpůsobovala novým podmínkám a adekvátně reagovala na možné příležitosti. Vedle tradičního chápání zdrojů podniku (půda, práce, kapitál) je čím dál častěji zdůrazňován vliv *informací* jako konkurenční výhoda.

Vytyčeným cílem diplomové práce je nastínění základních teoretických poznatků a následná analýza informační strategie v zemědělském podniku LUKROM, spol. s r.o. Hlavní směr, kterým se rozbor bude vyvíjet, je určení stupně vývoje, v němž se informační strategie v současném okamžiku nachází, posouzení jejího fungování a stanovení případných nedostatků a rizik. Komplexnost informační strategie znamená, že každý subjekt má odlišné požadavky a předpoklady na její integraci, a proto je nezbytné k ní přistupovat individuálně, a posoudit oblasti, které jsou pro podnik směrodatné. Výstupem celé práce je shrnutí získaných informací o aktuální situaci ve společnosti a navržení adekvátních řešení, které jsou vyčísleny také v rovině nákladů.

Práce je rozdělena do dvou hlavních oblastí – teoretická a praktická. V první části jsou zpracovány hlavní směry problematiky informační společnosti, což zahrnuje současný vývoj a změny v podnicích, informační hrozby, situaci v České republice a další podbody. Část praktická je tvořena popisem vybrané společnosti a jejími charakteristikami,

zpracování výsledků dotazníkového průzkumu a náměty pro management pak uzavírají tuto kapitolu. Obě části jsou kombinací objektivně získaných dat z různých zdrojů a subjektivních názorů a postojů autorky.

K získání potřebných informací byla použita metoda dotazníkového šetření, která má své opodstatnění v provádění průzkumu napříč celou firmou, tzn. všemi úrovněmi organizační struktury. Dalším rozhodujícím faktorem byla následná emailová komunikace s respondenty, kdy dotazník je nejschůdnější formou k získávání potřebných informací.

2 TEORETICKÁ VÝCHODISKA INFORMAČNÍ STRATEGIE

2.1. Informační společnost

Na počátku třetího tisíciletí se transformuje společnost do tzv. společnosti informační, která je výsledkem působení rozvoje informačních technologií a jejich zpřístupnění široké veřejnosti, rostoucího významu informací a rychlé a poměrně jednoduché cesty k jejich získání a přenosu. Nová éra přináší nepřeberné množství příležitostí, ale na druhé straně také rizika a hrozby. Směrodatné v konkurenčním prostředí je pak fakt, jak se s novými podmínkami jednotlivé podniky vyrovnají a jak rychle implementují změny do svých rutinních činností.

2.2. Informatizace společnosti

Jedná se o proces, který je dalším vývojovým stupněm po etapě industrializace. Kritériem úrovně informační společnosti je především rozsah, obsah, kvalita, užitečnost a dostupnost informací, informačních zdrojů a informačních služeb. Základem informatizace je intenzivní rozvoj elektroniky, informačních a komunikačních technologií. Důležitým prvkem v této společnosti bude osvojování si nových znalostí, které jsou výsledkem analyticko-syntetického vyhodnocování informací, a dále osvojování si zkušeností, jako výsledek praktického využívání vědomostí (Vymětal, Diačiková, Váchová, 2006).

Konečným cílem informační společnosti je zlepšení kvality života, zlepšení efektivnosti činnosti podnikatelských, rozpočtových a společenských organizací a posílení vzájemné soudržnosti lidí a národů (Vymětal, Diačiková, Váchová, 2006).

Základní charakteristiky informační společnosti (Vymětal, Diačiková, Váchová, 2006):

- vznik kvalitativní přeměnou industriální společnosti,
- nositelem inovačních změn a výchozím zdrojem rozvoje jsou informace a znalosti,
- probíhá intenzivní informatizace celé společnosti především rozvojem informačních a komunikačních technologií,

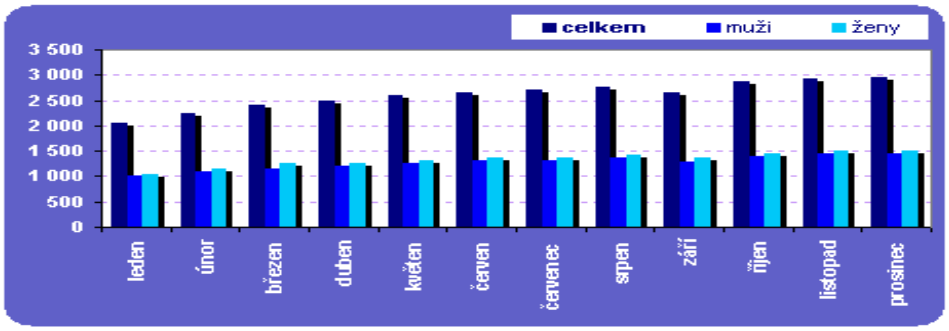
- vyžaduje se znalost práce s informacemi celé společnosti, znalostmi i zkušenostmi a související změny v myšlení, jednání i organizování podnikatelských subjektů,
- objem informací se každých tři až pět let násobí,
- zostřuje se konkurenceschopnost,
- nejvýznamnější oblastí se stává management informací a znalostí,
- rozhodujícím faktorem pro podnikatelskou sféru se stává produktivita znalostí a znalostních pracovníků,
- rozvíjí se informační ekonomika,
- významně se zvyšuje závislost na elektronizaci života, se všemi pozitivními i negativními důsledky,
- výrazně se mění pracovní prostředí, pracovní podmínky, pracovní návyky, rozvíjí se pracovní činnost v domácím prostředí,
- společnosti výrazně dominuje uchovávání informací v elektronické podobě a elektronická komunikace,
- proces učení se a jeho zvládnutí je důležitější než samotná výplň tohoto procesu.

2.3. Sociální sítě

Bezpochyby zažívají sociální sítě v současné době velký boom. Facebook může být jasnou jedničkou, ale není jediný – ještě před několika lety neexistující sociální sítě jsou součástí denního života 600 milionů lidí po celém světě (Dočekal, 2011). Z pohledu firem to znamená jednoznačnou výzvu, jež spočívá ve využití potenciálu právě sociálních sítí a neustále narůstajícího počtu uživatelů.

2.3.1. Uživatelé Facebooku v ČR

Uživatelů Facebooku v České republice bylo k prosinci 2010 bezmála 3 miliony, tedy nárůst téměř milionu uživatelů oproti stavu z ledna 2010. Mírně převažují ženy nad muži; svůj profil na Facebooku vlastnilo v prosinci cca 1,51 mil. žen oproti cca 1,45 mil. mužů (Uživatelé facebooku v České republice).



Obrázek 2-1 Uživatelé facebooku v České republice (2010)

Zdroj: ČSÚ

Dvanáctiměsíční období (leden-prosinec) v roce 2010 zaznamenalo rapidní nárůst uživatelů v ČR na téměř tři miliony, což je 28 % podíl celkové populace ČR. Tento fakt je významný především pro podniky, které by měly reagovat na měnící se mikroprostředí a přizpůsobovat tak své činnosti ve vztahu k zákazníkům i konkurenci.

2.3.2. Sociální sítě a firemní marketing

Dle Dočekala (2011) se sociální sítě staly magnetem pro firemní marketing a výsledkem je to, že přes polovinu uživatelů sociálních sítí se na nich spojuje se značkami, 36 % z nich se na svých účtech věnuje právě značkám. Pro spotřebitele je ale e-mail stále jasnou volbou, pokud se na něco chtějí zeptat nebo chtějí značce něco sdělit, sociální sítě jsou tak výrazně úspěšné pouze v šíření informací a povědomí o značkách – pouze 42 % se značkou komunikuje na sociální sítí. Nejvíce sledovanými značkami na sociálních sítích jsou média a zábava (50%), móda a luxusní zboží (45 %), jídlo a maloobchod (43 %), cestování (35 %) a sport (28 %).

Proč se stávají fanoušky	
Zákazník	46%
Doporučení od přátel	29%
Pozvánka od kontaktu ze sítě	28%
Vyhledávání	27%
Inzerce na sociálních sítích	26%
Inzerce na internetu	22%
Zájemce o koupi	22%
Pozvánka od značky	18%
Klasická inzerce	18%

Tabulka 2-1 Procentuální zastoupení možných způsobů stát se fanouškem

Zdroj: Dočekal

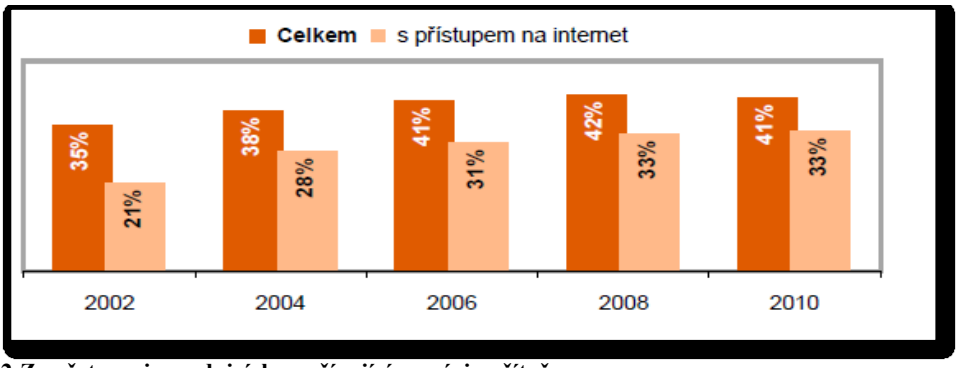
Tabulka přibližuje způsoby, jak se stát fanouškem dané značky. V popředí figuruje s velkým procentuálním odstupem „Zákazník“. Z toho vyplývá, že existují mezery ve zdokonalení a maximálním využití potenciálu sociálních sítí ze strany firem.

2.4. Změny v podnicích

Informatizace společnosti má zásadní vliv na podniky a charakter jejich fungování. Pakliže chce firma zůstat v poli konkurenceschopnosti, je nezbytné sledovat současné trendy a reagovat na měnící se podmínky. Současná doba je charakteristická svou dynamičností a neustále se rozvíjejícím prostředím, proto je podstatné, aby podniky tuto skutečnost akceptovaly a chápaly ji jako výzvu, nikoliv jako nutnost přizpůsobovat se a neustále měnit své dosavadní návyky a činnosti.

2.4.1. Využití výpočetní techniky zaměstnanci při práci v ČR

V níže uvedeném grafu jsou znázorněny informace o podnikovém využití počítačů, které byly získány Českým statistickým úřadem (Informační společnost v číslech).



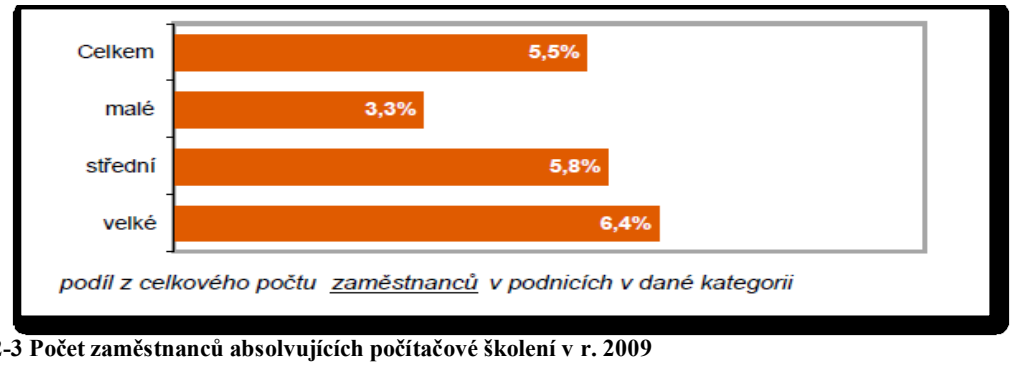
Obrázek 2-2 Zaměstnanci v podnicích používající v práci počítač

Zdroj: ČSÚ

V grafu můžeme sledovat rostoucí trend v celkovém využití počítačů, které představovalo v roce 2002 35% a v roce 2010 41%. Nárůst o šest procent však není nijak rapidní, což může svědčit například o nedostatečném přizpůsobení se nebo nedostatku finančních prostředků. Významnější posun se odehrál ve využití internetu, jenž představoval vzestup během osmi let dvanáct procent.

2.4.2. Absolvování zaměstnaneckého počítačového školení

Grafické pojetí procentuálního zobrazení počtu zaměstnanců, kteří absolvovali počítačové školení, přibližuje výsledky za rok 2009 (Informační společnost v číslech).



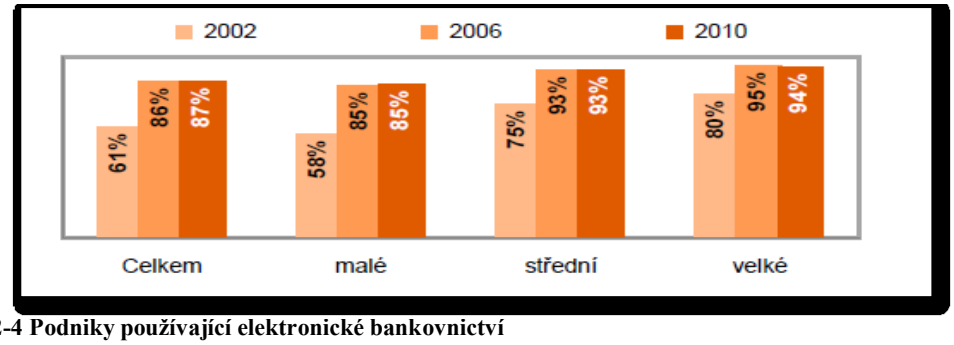
Obrázek 2-3 Počet zaměstnanců absolvujících počítačové školení v r. 2009

Zdroj: ČSÚ

Jak můžeme vyčíst z grafu, tak je více než patrné, že školení zaměstnanců v oblasti počítačové problematiky je nedostačující. Je podstatné, aby podnik rozvíjel a prohluboval poznatky v oblasti počítačů, technologií, bezpečnosti a ochrany firemních informací.

2.4.3. Podniky používající elektronické bankovnictví

Současná situace nabízí nejen podnikům, ale i veřejnosti možnost využívání elektronického bankovnictví, které spoří čas a poskytuje okamžité informace o stavu našich financí. Vyvstává ale i otázka bezpečnosti a snadnějšího zneužití uložených peněžních prostředků.



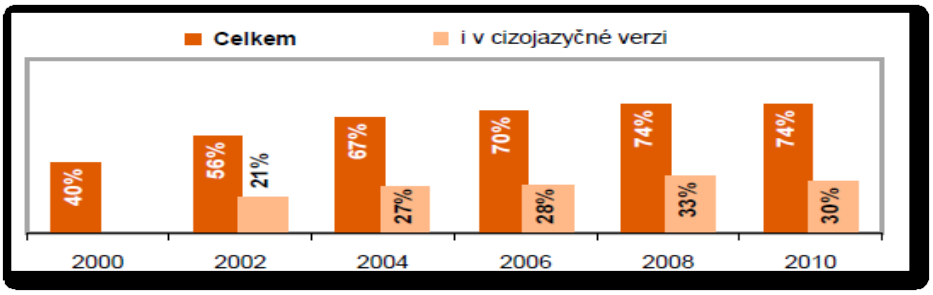
Obrázek 2-4 Podniky používající elektronické bankovnictví

Zdroj: ČSÚ

Z grafického znázornění vyplývá růst mezi jednotlivými obdobími ve čtyřletých intervalech. Celkový posun je o 26%, kdy největší skok byl zaznamenán u malých podniků (27%).

2.4.4. Podniky s webovými stránkami

Propagace organizace a zpracování webových stránek by měly podniky v současnosti považovat za samozřejmost. Důležitá je také image stránek, přehlednost, služby, marketing webových stránek a další.



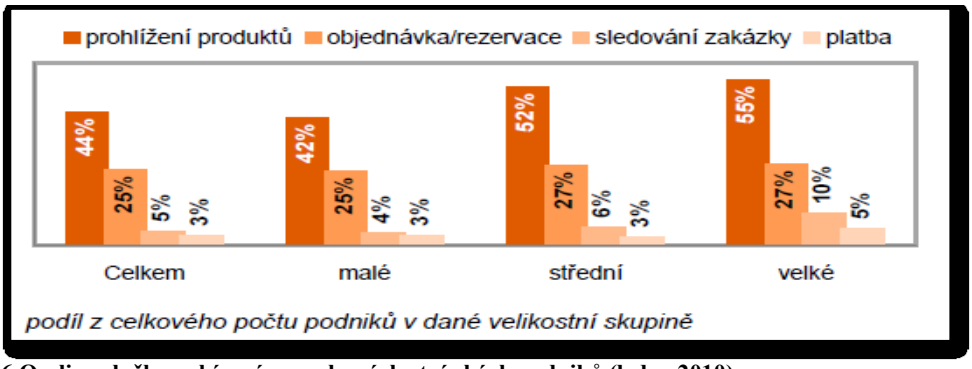
Obrázek 2-5 Podniky s webovými stránkami

Zdroj: ČSÚ

Vizualizace výše uvedeného procentuální vyjádření počtu podniků s webovými stránkami má charakter růstu v jednotlivých dvouletých etapách, přesto se domnívám, že v roce 2010 je 74% poměrně nedostačující vzhledem k současným požadavkům a celkovému rozvoji technologií. 30 % verze webovým stránek v cizím jazyce také neodpovídá kritériím, pokud chce firma konkurovat nejen v tuzemsku.

2.4.5. On-line služby nabízené podniky na webových stránkách

Nárůst nových způsobů pro zviditelnění se, oslovení nových zákazníků, poskytování služeb novými prostředky a další příležitosti jsou nepopiratelnou výhodou rozšiřování informační společnosti. Na druhou stranu s sebou nese pochopitelně i rizika a hrozby, které je zapotřebí ošetřit a minimalizovat.



Obrázek 2-6 On-line služby nabízené na webových stránkách podniků (leden 2010)

Zdroj: ČSÚ

Z celkového přehledu všech typů společností máme k dispozici data, která popisují stav jednotlivých charakteristik – prohlížení produktů, objednávka/rezervace, sledování zakázky, platba – za leden roku 2010. Nejvyšší podíl 44% zastupuje „prohlížení produktů“, „objednávky a rezervace“ dosahují 25% a „sledování zakázky a platba“ jsou více než zanedbatelné. Ať se jedná poté o velké či malé podniky, pak oba nemají uspokojivé hodnoty v právě těchto dvou posledních aspektech. Soudobá situace ale vyžaduje rozšiřování těchto služeb, které umožňují zákazníkům větší přehlednost a časovou úsporu.

2.5. Nedostatky v České republice

Ve studii s názvem „Digitální cesta k prosperitě“ (Voříšek, Novotný a kol.) zazněla mnohá zjištění, která nejsou pro Českou republiku příliš příznivá. Několik významných postřehů obsahuje následující část.

V digitální vzdělanosti[1] obyvatelstva Česká republika výrazně zaostává za většinou evropských zemí. Ze všech občanů EU starších 16 let nemá žádné počítačové dovednosti 36 % obyvatel. Takřka polovina (45,5 %) Čechů neumí vůbec zacházet s počítačem. Nedostatečná digitální vzdělanost přitom přímo ovlivňuje schopnost využívat potenciál ICT (*Informační a komunikační technologie*) pro rozvoj konkurenceschopnosti státu. Mezinárodní nezisková organizace ECDL Foundation prováděla každoroční analýzu počítačové gramotnosti[2] obyvatelstva v cca 139 zemích. Česká republika je v mezinárodním srovnání zemí z roku 2009, které přijaly koncept ECDL, na 37. místě. Mezi nejlepšími se umístily Irsko, Rakousko a Švédsko, před námi jsou mimo jiné Kypr, Slovensko, Rumunsko nebo Libye. Srovnatelného umístění jako ČR dosáhla například Zimbabwe (Chábera, 2011). Vzhledem k neustále se transformující prostředí je dalším stupněm v oblasti gramotnosti tzv. „informačně bezpečnostní gramotnost“, která klade důraz na ochranu dat a informací.

[1] Základní úroveň digitální vzdělanosti zahrnuje sledování základních počítačových dovedností (e-skills) a představuje základnu zvládání elementárních činností, které umožňují ovládat výpočetní techniku. Jde o dovednosti „Kopírování/ přesouvání souborů/složek“, „Kopírování/ vkládání dat v rámci dokumentu“, „Základní výpočty v tabulkových procesorech“, „Komprese/ zippování souborů“, „Připojování/ instalace hardwaru (tiskárna, modem,…) a používání programovacího jazyka k tvorbě programů“.

[2] Počítačová gramotnost zahrnuje kompetence, které umožní jedinci využívat nové technologie pro jeho profesní a osobní život v té míře, kdy se necítí komputerově handicapován, není za digitální přehradou a jeho osobní i profesní rozvoj prostřednictvím počítače je otázkou jeho volby (Sak, Saková, 2006).

V oblasti rozvoje technologické infrastruktury, obecných datových služeb, služeb e-government, e-commerce a e-business jsou na čele Norsko a Dánsko v rámci evropského srovnání. Česko spadá až do šesté skupiny zemí EU (z celkových osmi) spolu se Slovenskem, Slovinskem a Španělskem.

IT služby a telekomunikace (ICT služby) jsou jedním z nejefektivnějších odvětví hospodářství, srovnatelnou efektivitu má pouze finanční sektor a energetika. ICT služby se podílely v r. 2008 na HDP 3,81 %.

Na ICT pracovním trhu dlouhodobě převyšuje poptávka po ICT odbornících nabídku, a to zejména u pracovníků s vysokoškolským vzděláním. To se promítá i do průměrné mzdy těchto pracovníků, která výrazně převyšuje celorepublikový průměr.

2.6. Pozitivní a negativní aspekty informační společnosti

Rozvoj informační společnosti sebou přináší celou řadu příležitostí jak pro podniky, tak pro veřejnost a jednotlivce. Jedná se pak o rychlost přizpůsobení se novým podmínkám a využití svého potenciálu. Z druhého pohledu jsou však s pokrokem spojeny i negativní aspekty, které bude nutno ošetřit a minimalizovat.

2.6.1. Pozitivní aspekty

Mezi základní pozitiva patří dostupnost informací, jejich aktuálnost a úplnost, svoboda s nakládáním s informacemi, zvýšení informovanosti ve všech sférách profesionálního i soukromého života, poměrně levná výměna informací v celosvětovém měřítku, okamžitý přenos informace včetně její archivace, nové formy obchodu (*e-business*) a peněžních služeb (*e-banking*), virtuální podnikání a další (Vymětal, Diačiková, Váchová, 2006).

Díky informační společnosti se naskýtá firmám nová možnost využití technologií, což povede ke zkvalitnění, urychlení a zjednodušení podnikových činností. Jedná se například o oblasti marketingu, elektronického prodeje, výroby, bezskladového obchodování, elektronické publikování, práce na dálku (*teleworking*) a další (Vymětal, Diačiková, Váchová, 2006).

Rozvoj stávajících služeb bude mít zásadní vliv na informační průmysl a poskytne nové zdroje pro ekonomický růst. Elektronický obchod přinese možnost podnikání na globalizovaném trhu a může být jedním z nástrojů pro zvýšení konkurenceschopnosti společností (Informační společnost).

E-learning je pojem používaný k označení stále rozšířenějšího pronikání informačních technologií do oblasti vzdělávání. Pod *e-learning* spadají například nejrůznější multimediální výukové kurzy na CD-ROM či na internetu, videokonference sloužící ke zvyšování vzdělání, virtuální studium s využitím počítače, elektronická komunikace mezi studenty a učiteli a mnoho dalších nástrojů. Jednoznačné výhody z e-learningu pak nespadají pouze do oblasti distančního vzdělávání, ale platí i v rámci podniku jako v případě školení geograficky rozptýlených zaměstnanců či snižování nákladů na zapojení nových pracovníků do procesu (E-learning).

2.6.2. Fondy Evropské unie

Evropská unie se také zabývá vývojem informační společnosti a zaměřuje se na její rozvoj a podporu. Projekt z tzv. Horizontálních priorit 2004-2006 podopatření **4.2.1. - Podpora nadregionální infrastruktury CR SROP**, jehož cílem je např. vytvoření internetového informačního portálu o možnostech ubytování v městech ČR. Samotné vytvoření takového informačního zdroje má kladný vliv na informační společnost, "nutí" k užívání internetu a zvyšuje tak informační gramotnost obyvatelstva (Horizontální priority v projektové záležitosti).

Ze současných Programů 2007-2013 můžeme zmínit **1.1 Rozvoj informační společnosti ve veřejné správě**, jehož cílem je modernizace a zefektivnění činnosti a procesů v oblasti veřejné správy a navazujících veřejných služeb a územního rozvoje jako předpokladu pro vytvoření moderní občanské společnosti a zvýšení konkurenceschopnosti regionů a ČR jako celku (Rozvoj informační společnosti ve veřejné správě).

Evropská unie vyhlásila poslední možnost participace na **programu ICT** v podnicích do roku 2013. Jeho prostřednictvím mohou malé a střední podniky výrobního charakteru (kromě zemědělské prvovýroby, výrobců lodí, chemických vláken a několika dalších výrobních odvětví) získat 50-60% dotaci na nákup informačních systémů a široké škály k nim se vážícího HW a SW vybavení a příslušenství. Projekt lze realizovat od konce

ledna 2012 do konce roku 2014. Požádat o dotaci mohou i společnosti, které již získali finanční prostředky z některé z předchozích výzev (Financování z EU fondů, 2012).

2.6.3. Negativní aspekty

Míru působení negativních důsledků nelze v současné době ještě odhadnout či posoudit, ale již nyní můžeme s jistotou prohlásit, že informační společnost sebou nese i řadu nežádoucích aspektů jako určitá ztráta soukromí a sociálních vazeb, nebezpečí zahlcování informacemi, ztráta právního povědomí vyvolaná anonymitou přístupu na síť, zvýhodnění podmínek pro organizovaný zločin, některé problémy filosofického, morálního, zdravotního charakteru, problematika ochrany dat a informací, nevyhovující současný stav vzdělávacího systému atd. (Vymětal, Diačiková, Váchová, 2006).

Děti se setkávají s hraním her on-line s virtuálními protihráči nebo skutečnými spoluhráči, záměrně využívají internet, komunikují pomocí různých programů (ICQ, Skype), využívají sociální sítě (Facebook, Twitter), postupně ovládají mobilní telefony, bezdrátovou komunikaci a další technologie. V kombinaci s nevyzrálostí osobností se tyto symptomy stávají nebezpečné, pokud nedochází ke zpětné vazbě a sebekontrole. Nový psychologický úkaz se nazývá „*Flow fenomén*“, kdy se jedná o formu pohlcení, splynutí s prostředím při počítačové hře. Jedinec přestává vnímat prostor i čas (Negativa vstupu ICT do vzdělání).

Počítačová kriminalita i díky anonymitě kybernetického prostoru narůstá do rozměrů, kdy se stává nejvíce nebezpečnou kriminální hrozbou, jaké bylo nutné čelit. Tato skutečnost nezůstává skryta ani před teroristy (Pinkava, 2010).

Je zaznamenáván rapidní nárůst neschopnosti racionálně využívat informační zdroje. Místo informačního komfortu se hovoří o prostředí zamořeném informačním smogem, kdy uživatelé jsou bezpochyby vystaveni stresům. Informační smog má podobu např. zbytečných a nepoužívaných počítačových výstupů (papír, počítačové soubory), množství nevyřízených e-mailů, stohů nepřečtených odborných časopisů, nezpracovaných zápisů z porad a zasedání (Keřkovský, Drdla, 2003).

2.7. Informační exploze a exformace

Podmíněnost úspěchu jak na úrovni firem, tak na úrovni jedince je schopnost najít, analyzovat a umět používat informace. Ty ale vznikají mnohem rychleji a ve větších objemech, než je schopnost člověka je nalézt, studovat je a současně jim porozumět. Tento jev je označován jako informační přehlcení neboli exploze (Sklenák, 2001). V současné době dochází k rozšíření problémů s nadbytečnými daty a informacemi, tedy s jakýmsi informačním odpadem, pro který navrhl americký politik Al Gore termín "exformace" (Informační exploze a exformace).

2.7.1. Informační exploze

Dle Viléma Sklenáka (2001) způsobuje informační přehlcení neschopnost vytěžit potřebné znalosti z nezměrného kvanta informací. Přehlcení nastává v případě, když člověk:

- nedokáže porozumět dostupným informacím,
- cítí se zavelen množstvím informací, které má vstřebat,
- nemá tušení, zda určité informace existují,
- nemá tušení, kde informace hledat,
- ví, kde informace hledat, ale neví, jak se k nim dostat.

V souvislosti s Internetem je zdůrazňována verifikace přesnosti informací, jelikož právě internetové zdroje mohou potenciálně obsahovat data nekonzistentní, chybná nebo zbytečná. Stejně tak mohou být nalezeny informace konfliktní či nepožadované. Přesnost výsledků je pak ovlivněna dvěma faktory. Prvním je pohled samotného uživatele a druhým funkční schopnosti používaného systému (Sklenák, 2001).

Společnost EMC Corporation představila výsledky studie Digital Universe organizace IDC s názvem „*Extracting Value from Chaos*“ (Získávání hodnoty z chaosu), kterou sponzorovala. Studie došla k závěru, že objem informací na světě se každé dva roky více než zdvojnásobí a roste tak rychleji, než udává Moorův zákon[3] – v roce 2011 má být vytvořeno a replikováno neuvěřitelných 1,8 zetabajtů[4] dat. Takové množství by například

[3] Každé dva roky se množství tranzistorů na počítačových čipech zdvojnásobí, a tak se zvýší i výkon počítačů.

[4] Jeden zetabyte (ZB) odpovídá 10 na 21tou bytů.

vytvořili obyvatelé Spojených států, kdyby po dobu 26 976 let zveřejnili každou minutu 3 příspěvky v síti Twitter. Odpovídá to také více než 200 miliardám filmů ve vysokém rozlišení (každý o délce dvě hodiny). Zhlédnutí by jednomu člověku při nepřetržitém sledování trvalo 47 milionů let. Od roku 2005 navíc každoroční investice podniků do oblasti digitálního světa, tedy cloudových řešení, hardwaru, softwaru, služeb a personálu potřebného k vytváření, správě a ukládání těchto informací a ke generování příjmů na jejich základě, vzrostly o 50 % na 4 biliony USD (Objem dat na světě se každé dva roky více než zdvojnásobí).

Na každých 1000 duševně pracujících připadá ztráta ve výši 5,7 miliónů dolarů v podobě ztraceného času přeformátováváním informací mezi aplikacemi. 42 % manažerů přiznává, že neodvratně používají špatná data alespoň jednou týdně (Chytrá rozhodnutí vedoucí k optimalizaci výkonu).

2.7.2. Nová data – nové příležitosti

Všechna tato nová data jsou doprovázena problémy - zároveň skýtají vynikající příležitost k získávání nových informací a věcného přehledu. Podniky a vládní organizace projevují zájem o metody třídění dat, identifikaci a propojování dílčích informací, aby dosáhly lepších obchodních výsledků. Úspěšné organizace zjišťují, že potřebují pro řešení informační exploze změnit své uvažování a využít příležitosti k posunutí svého výkonu na další úroveň (Chytrá rozhodnutí vedoucí k optimalizaci výkonu).

Management podniku musí tedy co nejrychleji reagovat na měnící se podmínky a sledovat momentální trendy a možnosti ve zpracování dat a informací, které umožní snadnější orientaci v jejich získávání a třídění.

2.7.3. Exformace

S postupem času se zvýšila naše závislost na všech formách informací, ale přitom si téměř nikdy neklademe otázku, zda je tato závislost prospěšná a zda nemohou mít informace i negativní účinek na náš život. Hrozí totiž úniky „toxických“ informací (např. návody na výrobu jaderných zbraní, otravných látek, drog apod.), rozvíjí se průmyslová špionáž a jiné (Informační exploze a exformace).

Pojem exformace použil rok před Albertem Gorem dánský popularizátor vědy a spisovatel Tor Nørretranders k označení sdíleného kontextu v komunikaci. Exformace je tedy všechno, co reálně neříkáme, ale máme to v mysli, když mluvíme nebo před tím, než něco řekneme (Nørretranders in Tomáš, 2010). Vzhledem k významu latinské předpony *ex* se Nørretrandersovo užití termínu exformace k popsání kontextu ležícího vně informace a komunikace jeví jako logičtější než Gorovo využití pojmu k označení informačního odpadu, ač ho lze chápat jako nevyužitelná data uložená mimo lidský mozek. Častěji užívaným výrazem pro nepotřebné či přebytečné informace umístěné mimo lidské vědomí se nakonec stalo slovní spojení **data smog**, jenž jako nepotřebné informace - nevítanou a nečekanou součást naší atmosféry, tedy velmi podobně jako vysvětluje svůj termín exformace Gore, definoval David Shenk v knize *Data Smog: Surviving the Information Glutc* v roce 1997 (Shenk in Tomáš, 2010).

2.8. Informační hrozby

Moderní informační a komunikační technologie se vyznačují celou řadou vlastností, které znamenají nejenom výhodu pro bezúhonného uživatele, ale i pro zločince (a často zároveň nevýhodu pro specializované bezpečnostní složky). Z tohoto důvodu se jedná o jednu z klíčových bezpečnostních výzev současnosti (Bezpečnostní hrozby).

2.8.1. Základní hrozby

Dle Jirovského (2007) můžeme rozlišit čtyři základní skupiny možných hrozeb, které odrážejí hledisko bezpečnosti informačních systémů:

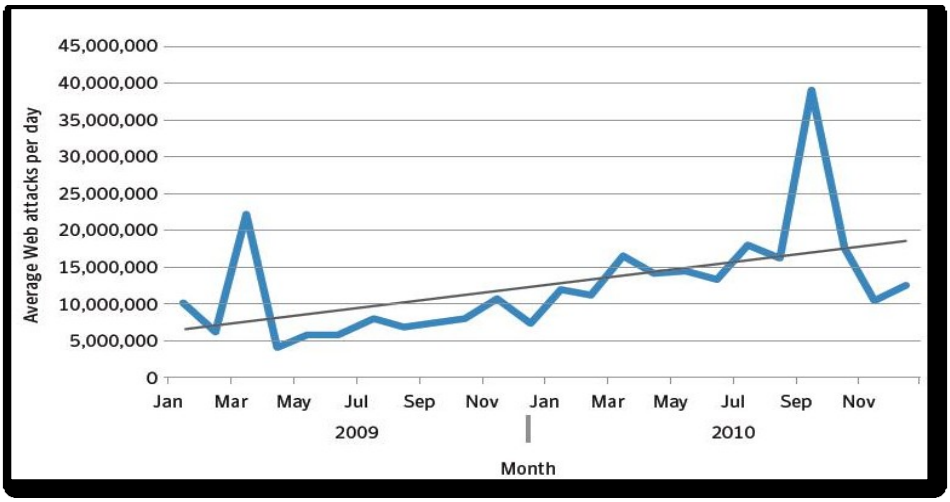
- **Únik informace** neboli případ, kdy informace důvěrného charakteru je prozrazena neautorizovanému subjektu nebo je jím odhalena. Únik informace může pak vést k přímým útokům se značným dopadem.
- **Narušení integrity** zahrnuje porušení konzistence dat, kdy může dojít k vytvoření nových dat či změně nebo vymazání stávajících dat neautorizovaných subjektem.
- **Potlačení služby**, ke které dochází v případě, kdy je úmyslně bráněno v přístupu legitimního subjektu k informacím nebo jiným systémovým zdrojům.
- **Nelegitimní použití** znamená, že zdroj je používán neautorizovaným subjektem nebo neadekvátním způsobem.

2.9. Kybernetická kriminalita

Jedná se o takovou činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti. Tato kriminalita může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se činnost odehrává (Jirovský, 2007). Mezi základní typy útoků patří kybernetické pronásledování, kyberterorismus, kybernetická pornografie, kybernetická krádež, kybernetický podvod, kybernetické praní špinavých peněz a další (Ministerstvo vnitra české republiky).

2.9.1. Finanční ztráty díky internetové kriminalitě

S nárůstem internetové kriminality přibývají podnikům výdaje spojené s odstraňováním škod, zaváděním bezpečnostních systémů, vzděláváním zaměstnanců a další.



Graf 2-1 Finanční ztráty díky internetové kriminalitě

Zdroj: JustIT.cz

Na vertikální ose jsou zaneseny hodnoty průměrných denních webových útoků a na horizontální pak jednotlivé měsíce za období 2009 a 2010. Z grafu je patrný rostoucí trend finančních výdajů a také průměrný nárůst denních útoků. Podniky, které chtějí uchránit svá data před případným útokem, musejí investovat nemalé peněžní prostředky do ochranných systémů a především vzdělávacích programů svých zaměstnanců na všech úrovních.

2.9.2. Předpoklady kybernetické kriminality

Moderní (informační a komunikační) technologie umožňují globální dostupnost. To zvětšuje vzdálenost mezi pachatelem a obětí, a tím dochází ke zjednodušení činnost útočníka ze vzdáleného místa. Další nespornou výhodou je anonymita a rychlost. Ta zajišťuje kriminálním skupinám velmi rychle přenášet (kopírovat, ničit, pozměňovat) velké objemy dat. Ceny výpočetní techniky navíc neustále klesají, a tak jsou dosažitelnější pro stále širší skupinu obyvatel. Ovládání takové techniky nevyžaduje zvláštní vzdělání. Existuje také značná asymetrie mezi ”útočníky” a ”obránci”. Útočník je vždy tím, kdo volí cíl, okamžik a metodu útoku. Protiopatření, která by útok proti kybernetickým systémům ztížila, jsou oproti tomu velmi nákladná (Kybernetické hrozby).

Počítačová a informační kriminalita se vymyká běžným vyšetřovacím postupům (Kybernetické hrozby):

- Digitální stopy jsou vysoce objemné, značně proměnlivé a mohou být rozptýleny na velkém geografickém prostoru (”všude a nikde”).
- Ne vždy je bezproblémové jako důkazní materiál zajistit napadený hardware (počítače a další techniku), protože by to znamenalo další ztráty pro již tak poškozené oběti.
- Škody, resp. ztráty, způsobené kybernetickou kriminalitou, se obtížně zjišťují, resp. vyčíslují (zejména co se týče kriminality, související s duševním vlastnictvím).
- K analýze či dešifrování digitálních stop je často nutný specializovaný a certifikovaný software či hardware, který bezpečnostní složky postrádají.
- Zákony, postihující kriminální chování v uvedené oblasti, jsou stále ve vývoji a existují spíše ve fragmentech.
- Pravidlem je rovněž obecně nízká úroveň akceptace digitálních stop v právní praxi.

2.10. Sociální inženýrství

Na webových stránkách *PCWorld* v článku z června 2012 „Co je sociální inženýrství?“ je tato problematika specifikována jako způsob manipulace lidí za účelem provedení nějaké akce nebo získání určité informace. Na základě některých uměle vytvořených indicií se člověk domnívá, že komunikuje s někým důvěryhodným, přičemž v pozadí stojí právě podvodník. Tato technika má ostatně kořeny i v klasických podvodech reálného světa (falešní výběrčí doplatků za vodu, plyn či elektřinu). Sociální inženýrství je

aplikací netechnickým věd – psychologie a sociologie, které slouží k překonávání bezpečnostních bariér, a zabývá se sledováním a analyzováním typických vzorců chování (stereotypů) a jejich možnou aplikací. Jako příklad některého ze stereotypů je fakt, že 40-60 % uživatelů volí jako svůj základ hesla jméno nebo příjmení, které následně modifikují velkými písmeny (začátek/konec) a číslicemi (většinou konec) do minimální požadované délky (Slinták, 2009).

Mezi základní techniky jsou uváděny například sabotáž (napadení web serveru apod.), inzerce (útočník nabízí své služby jako konzultant), phishing, sociální sítě, pomocí telefonátu a další (Slinták, 2009).

Základní doporučení jak pro sféru uživatelů, tak i jednotlivé podniky k ochraně proti sociálnímu inženýrství je:

- neotvírat jakýkoliv podezřelý email
- banka ani žádná jiná instituce nekontaktuje své klienty o změně hesla přes email
- třídit separátně dokumenty s citlivými firemními či osobními daty určené k likvidaci
- provádět pravidelná školení

2.11. Phishing

Podstatou metody usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtů apod. za účelem jejich pozdějšího zneužití, je vytvoření podvodné zprávy šířené například elektronickou poštou, s pomocí níž se pachatel snaží zmíněné údaje z uživatele vylákat (Jirovský, 2007). Nemusí jít jenom o účty přímo bankovní, ale také ostatních organizací, kde dochází k manipulaci s penězi nebo je možné jakýmkoliv způsobem zneužít jejich služeb. Příkladem může být PayPal, eBay, Skype, Google.

Základní znaky phishingového e-mailu:

- Snaží se vyvolat dojem, že byl odeslán organizací, z jejíchž klientů se snaží vylákat důvěrné informace. Toho se snaží docílit grafickou podobou e-mailu a zfalšováním adresy odesílatele.

- Text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, výzkum klientské spokojenosti nebo jako elektronický bulletin pro klienty.
- V textu zprávy je link, který na první pohled většinou vypadá, že směřuje na stránky organizace (banky). Při jeho bližším prozkoumání zjistíte, že ve skutečnosti odkazuje na jiné místo, kde jsou umístěné podvodné stránky.

Phishing není žádnou novinkou, první záznamy jsou z poloviny 90. let minulého století. Masově se rozšířil počátkem tohoto století. V březnu 2006 byl zaznamenán první český útok, tentokrát na klienty CityBank. V říjnu 2006 byl proveden první útok na klienty České spořitelny. Až na pár výjimek byl napsán poměrně dobře česky. Od počátku roku 2008 začaly masívní útoky na klienty České spořitelny. Nejdříve to byly úsměvné pokusy s neumělou češtinou. S největší pravděpodobností se jednalo o strojové překlady. Další pokusy varovaly před neprovedenou transakcí nebo slibovaly odměnu za vyplnění dotazníku. Všechny tyto podvodné e-maily byly psány buď anglicky, nebo nepovedenou češtinou. Zlom nastal až ve chvíli, kdy podvodníci použili velmi jednoduchý trik. Text jednoduše okopírovali přímo ze stránek České spořitelny. Zneužili aktualitu, která varuje před podvodnými e-maily.

Dne 15. 11. 2011 se objevil v emailových schránkách "pěkně" propracovaný podvodný e-mail, který se pod příslibem elektronického výpisu snaží vylákat přístupová hesla k účtu klientů ING-BANK. Náhled do tohoto phishingového pokusu je umístěn v příloze č. 1.

Naštěstí v současné době více a více webových stránek integruje k ověření uživatele ještě jednu úroveň vedle přihlašovacího jména a hesla. Jedná se o element, který je známý jen uživateli samotnému. Může se jednat například o zaslání speciálního kódu na mobilní telefon (Mustaca, 2012).

2.12. Pharming

Pharming využívá speciální počítačové programy, které uživatele při přihlášení do internetového bankovnictví přesměrují na stránky, jež sice vypadají jako stránky jeho banky, ale ve skutečnosti jsou pouze jejich napodobeninou. Zde pak klienta požádají o zadání všech přihlašovacích hesel a kódů. Pokud tak klient učiní, mohou se neoprávnění

uživatelé přihlásit do internetbankingu pod jeho jménem, a pokud klient nemá nastaveno další zabezpečení (např. potvrzování transakcí pomocí autorizační SMS nebo klientský certifikát), mohou mu nepozorovaně převést peníze z jeho účtu (Phishing a pharming).

Pharming v „globálním“ měřítku spočívá v tom, že útočník neoslovuje přímo jednotlivé uživatele služby, ale napadne vybraný DNS server[5]. Druhou metodou je tzv. „lokální“ pharming, která je založena na útoku proti jednotlivým počítačům (Bednář, 2007).

Pharming je mnohem nebezpečnější než phishing uvedený v předchozím odstavci a možnosti správců uživatelských PC a samotných uživatelů postupovat proti pharmingu založenému na napadení DNS serveru jsou v podstatě minimální. Ochrana proti lokální formě útoku je založena především na aktivním, správně nastaveném a hlavně aktuálním antivirovém programu. Dalším důležitým aspektem je informování uživatelů a určitá hygiena práce s počítačem. Uživatelé by měli vědět, že nesmí bezhlavě klikat na odkazy v emailech, stahovat z Internetu neznámé aplikace a jiné (Bednář, 2007).

2.13. Malware

Malware je program určený ke vniknutí do počítačového systému a k jeho poškození. Pod souhrnné označení malware se zahrnují počítačové viry, trojští koně, spyware - program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele či adware - znepříjemňuje práci s nějakou aplikací reklamou (Tvrdíková, 2008).

Podle poslední uveřejněné statistiky počítačových hrozeb patří druhá příčka právě malwaru s názvem Dorkbot (3,43 %), který se také šíří především přes vyměnitelná média a v počítači shromažďuje uživatelská jména a hesla, která uživatel vyplňuje na určitých webových stránkách. Všechna data pak virus odesílá útočníkovi přímo do počítače (Počítačovým hrozbám kralují viry přes USB flash disky, 2012).

[5] DNS server je hierarchický systém doménových jmen, který slouží jako distribuovaná databáze síťových informací.

2.14. Kyberválka

Ruský odborník Eugene Kaspersky prohlásil na londýnské konferenci o kybernetické bezpečnosti (2011), že svět je velice blízko kyberterorismu. Evropské firmy působící v jaderném průmyslu a jiných klíčových odvětvích se v minulých měsících staly terčem útoku nového počítačového viru zvaného *Duqu*, shromažďujícího citlivá data. Dále byly zveřejněny detaily o počítačovém programu *Nitro* určeném k poškození počítačových sítí chemických a jiných společností pracujících pro ministerstva obrany v USA, Británii a Bangladéši. Podobné ataky se stávají stále častějšími, a proto se mnozí odborníci domnívají, že brzy zasáhnou i klíčové státní infrastruktury.

Stejný skeptický názor zastává i vývojář antivirů a šéf AVG VirusLab Pavel Krčma. Hackeři každoročně kradou údaje velkým firmám, jen letos napadli třeba společnost Sony nebo internetové stránky izraelské armády. Počítačová kriminalita je stále častější a zdaleka se netýká jen velkých firem. V současné době se na burzách prodávají balíky nevyžádané pošty, stejně jako čísla kreditních karet. V rozhovoru pro Lidové noviny dále uvedl, že kybernetické války již v podstatě právě probíhají. Příkladem je kauza posledního roku, počítačový červ *Stuxnet*, jehož cílem bylo napadnout a poškodit íránské zařízení na obohacování uranu. Existuje reálné podezření, že za tímto velmi nebezpečným kódem stojí vzhledem k náročnosti vývoje nějaký stát. Stejným případem jsou i pokusy o průnik čínských státních hackerů do sítí vládních organizací USA, kde obvykle pátrají po nějakých zajímavých materiálech.

Tomu, že se nacházíme na hranici kyberterorismu, resp. kyberválek či dokonce již za ní, nasvědčuje i nedávné rozhodnutí prezidenta USA Baracka Obami o přijetí směrnice, jenž upravuje pravidla kybernetických válek, které může americká armáda a tajné služby vést v zahraničí. Dokument Bílého domu vypočítává kybernetické nástroje, jichž může Pentagon použít v době míru a během vojenského konfliktu. Jde například o infikaci počítačovým virem nebo o kybernetický útok proti elektrické rozvodné síti nepřítele či proti jeho obranné infrastruktuře.

Výzkum společnosti Panda Security z roku 2008 informuje o napadení škodlivým softwarem, který se pokoušel získat citlivé zneužitelné osobní údaje uživatelů, téměř deseti miliónů počítačů. Zatímco v minulosti byla většina malwaru zaměřena na páchání přímé škody na datech, softwaru či hardwaru, v současnosti si autoři různých virů a červů

uvědomili, že zapojení počítačů do botnetů[6] a právě krádeže osobních informací mohou být vítaným zdrojem zisku. Je důležité si uvědomit, že vývoj útoků tohoto typu má exponenciální charakter a nástroje a možnosti se neustále zdokonalují a stávají se nebezpečnějšími. Časový úsek měnících se podmínek se zkracuje a vytváří tak obrovský tlak nejen pro podniky, ale i pro celou společnost.

2.15. Situace v České republice

Záznam interview z března 2010 s Alešem Špidlou, ředitelem odboru kybernetické bezpečnosti Ministerstva vnitra, pojednává o kybernetické bezpečnosti země, odkud nám hrozí největší rizika, jak jsou vůbec důležité sítě v ČR zabezpečeny a hrozby „kyberválky“. Hlavním problémem je roztříštěnost právního prostředí, proto je cílem vytvořit zákon o kybernetické bezpečnosti. Nejslabší místa vidí tam, kde neexistuje vědomí o těchto hrozbách. Další slabinou v ČR je neadekvátní přístup policie, který nezabezpečuje dostatečnou rychlost v případě skutečného ohrožení.

Nejčastějšími incidenty jsou návštěva infikované stránky a phishing, kdy útočník odešle nějakou falešnou zprávu, která se ale tváří jako oficiální zpráva například od banky. Nejznámější v Česku byl phishing na Českou spořitelnu (Krčma, 2011).

Od roku 2007 působí v českých podmínkách tým *CSIRT.CZ*, který je bezpečnostní složkou pro koordinaci řešení bezpečnostních incidentů v počítačových sítích. Cílem je pomáhat provozovatelům internetových sítí v České republice, zřizovat jejich vlastní bezpečnostní týmy a bezpečnostní infrastrukturu, řešit bezpečnostní incidenty a tím zlepšovat bezpečnost jejich sítí i globálního Internetu. *CSIRT.CZ* také pomáhá předávat hlášení o bezpečnostních incidentech správcům těch sítí nebo domén, z nichž incidenty pocházejí, ale které na stížnosti nereagují. V tomto směru tedy slouží jako jakýsi "institut poslední záchrany" pro případ, že jiné metody kontaktování správců selžou. Hlavním a nejdůležitějším cílem pro rok 2011 bylo úspěšně dokončit převzetí agendy a provozu *CSIRT.CZ* a to tak, aby služba v oblasti řešení a koordinace řešení bezpečnostních incidentů byla kontinuální, a pokračovat v mezinárodní i domácí spolupráci.

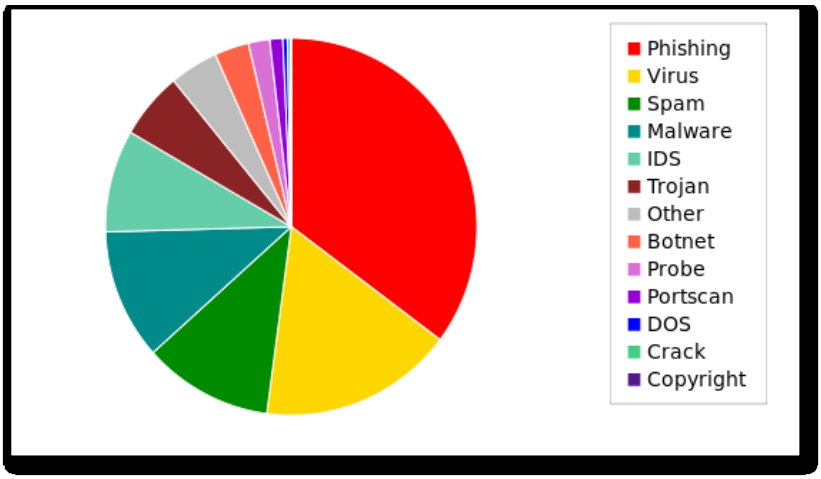
[6] Dnešní škodlivé kódy a červi často staví botnety, což jsou sítě propojených botů na zavirovaných počítačích (zotročená síť počítačů), kteří čekají na příkazy majitele a poté používají napadené počítače k jejich splnění.

Vláda České republiky uložila svým usnesením č. 205 ze dne 15. března 2010 zpracovat Strategii pro oblast kybernetické bezpečnosti, jejímž cílem je formulovat strategické oblasti, priority a cíle kybernetické bezpečnosti, které je nutné zavést do praxe v období let 2011 - 2015. Strategie stanovuje tyto hlavní prioritní oblasti v budování kybernetické bezpečnosti v České republice:

I. Koordinace a řízení rizik kybernetické bezpečnosti ČR.
II. Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti ČR.
III. Národní spolupráce v oblasti kybernetické bezpečnosti (veřejné, soukromé a akademické).
IV. Vytvoření legislativního rámce k posílení kybernetické bezpečnosti ČR, podpora a ochrana lidských práv a svobod.
V. Zvyšování povědomí a znalostí o kybernetické bezpečnosti ČR.
VI. Posilování kybernetické bezpečnosti v ICT veřejné správy a komunikační infrastruktury ČR.
VII. Posilování odolnosti proti narušení ICT systémů a proti kybernetickým útokům.

2.16. Druhy incidentů

Výchozí data pro zpracování statistiky jsou za období 1. 4. 2008 – 13. 11. 2011, která zpracoval tým *CSIRT.CZ*. V níže uvedeném koláčovém grafu jsou zachyceny informace o výskytu jednotlivých škodlivých incidentů.



Graf 2-2 Druhy jednotlivých incidentů za období 2008 – 2011

Zdroj: CSIRT.CZ

V grafu je téměř jedna třetina všech různorodých útoků v zastoupení phishingu. Velký podíl je také zaznamenám u různých typů virů, spamu, malware či Trojského koně. Ostatní skupiny škodlivého kódu zůstávají v menším procentuálním zastoupení.

Níže umístěná tabulka prezentuje výsledky průzkumu stavu informační bezpečnosti (ve firmách a institucích) v ČR (Tvrdíková, 2008).

	Typ	**Počet kladných odpovědí v % z celkového počtu respondentů**
Nejčastější bezpečnostní incidenty	nevyžádaný e-mail (spam)	86
	výpadek proudu	85
	porucha hardwaru	78
	počítačový virus	74
	chyba uživatele	59
Největší hrozby z hlediska informační bezpečnosti	internet a e-mail	58
	vlastní uživatelé	57
	vnější útočníci	30
	neexistence, nevhodnost bezpečnostní politiky	21
Ochranná opatření	firewall	93
	monitoring a kontrola virů	86
	směrnice pro užívání internetu	55
	formálně definovaná bezpečnostní politika ve formě dokumentu	48
	penetrační testování	18
	realizace procedur a opatření kontrolujících dodržování směrnic	14

Tabulka 2-2 Výsledky průzkumu stavu informační bezpečnosti ve firmách a institucích v ČR

Zdroj: Tvrdíková, 2008

V současné době vzrůstá počet i složitost útoků nejrůznějších forem. Internet v sobě skýtá poměrně snadnou cestu k potenciálním útokům, proto je podstatné, aby společnosti kladly důraz na bezpečnostní politiku, zpracování informační strategie, školení zaměstnanců i zvyšování povědomí o možných hrozbách atd.

2.17. Zvládání informačních hrozeb v organizaci

Zajištění bezpečnosti informací je komplexním a systémovým procesem, jehož cílem je nastartovat a udržet interní bezpečnostní kulturu organizace na úrovni, která vytváří dostatečnou bezpečnost informací v organizaci. (Vymětal, Diačiková, Váchová, 2006). Stále se opakuje situace, že není vytvořen speciální útvar pro informační

bezpečnost, ale tuto otázku řeší oddělení IT, navíc často velmi nízko umístěné v hierarchii organizace. V řadě organizací budování bezpečnosti skončí u vytvoření bezpečnostní politiky, která ale již nikdy není v praxi realizována. Z průzkumu také vyplynulo, že hlavním problémem nejsou peníze, ale nízké bezpečnostní vědomí v ČR, které ústí právě v nedostatečnou podporu ze strany vedení organizace (Brechlerová, 2005).

2.17.1. Právní předpisy

Právní systém obsahuje velké množství zákonů, vyhlášek, směrnic a norem, které se vztahují k informační bezpečnosti a to jak na úrovni České republiky, tak i Evropské Unie. ČSN BS 7799-2:2004 Systém managementu bezpečnosti informací - Specifikace s návodem pro použití je původně Britský standard – BS 7799, který se stal nejuznávanější normou v oblasti řízení informační bezpečnosti vzhledem k jeho vysoké kvalitě a srozumitelnosti (Standardy a doporučení). Další důležitou normou je ISO/IEC 27000, jejímž cílem je sjednocení požadavků, návodů a doporučení na systémy řízení informační bezpečnosti, které se vyskytují v různých normách (Seznam ČSN). Je nutné si uvědomit, že právní předpisy jsou pouze určitým teoretickým východiskem, ale samotná aplikace a dodržování nastavené bezpečnostní politiky je v rukou firem.

2.17.2. Etapy bezpečnostní politiky

Dle autorů Vymětal a kol. je možné rozčlenit jednotlivé kroky programu bezpečnostní politiky do sedmi etap:

1. **rozhodnutí managementu** – vyčlenění pověřených pracovníků (útvar bezpečnosti, bezpečnostní manažer), vyhrazení finančních prostředků, zodpovědnost za bezpečnost na nejvyšší úrovni, podpora systematičnosti trvalého řešení informační bezpečnosti, spolupráce s externími dodavateli prvků bezpečnosti,
2. **strategie informační bezpečnosti** – definování hlavních cílů (co a jak chránit), projekty a chronologie jednotlivých kroků, včetně návaznosti na celkovou bezpečnostní politiku organizace,

3. **analýza rizik** – analýza a posouzení reálných rizik, reálné zranitelnosti, specifikace ostatních méně pravděpodobných rizikových faktorů, návrh priorit rizik a opatření k jejich eliminaci,
4. **informační bezpečnostní politika** – definice všech východisek a cílů pro aktivity organizace v oblasti informační bezpečnosti, určení způsobů, jak bezpečnost řešit, určení pravomocí a zodpovědnosti,
5. **bezpečnostní směrnice a standardy** – zpracování bezpečnostních směrnic v rámci interní legislativy organizace,
6. **implementace bezpečnosti** – realizace bezpečnostních projektů, zajištění průběžného bezpečnostního vzdělávání, havarijní plánování a cvičení, zabezpečení připojení na internet a optimalizace využívání IT i IS, implementace infrastruktury veřejných klíčů,
7. **monitorování a kontrola** – dodržování přijatých pravidel a zásad, doplňování příslušných dokumentů, reakce na nově se objevující rizika, akceptování změny priorit organizace, doplňkové analýzy, realizace zpětné vazby.

Dokument „Bezpečnostní politika“ specifikuje povinnosti a odpovědnosti vedoucích pracovníků, správců systému, zaměstnanců podniku, poskytovatelů služeb v oblasti IT, organizační zajištění bezpečnosti informací, klasifikace jednotlivých úrovní informací, pravidla přístupu ke zdrojům podniku, definice pravidel externí komunikace, definice nouzových opatření (Vrana, Richta, 2005).

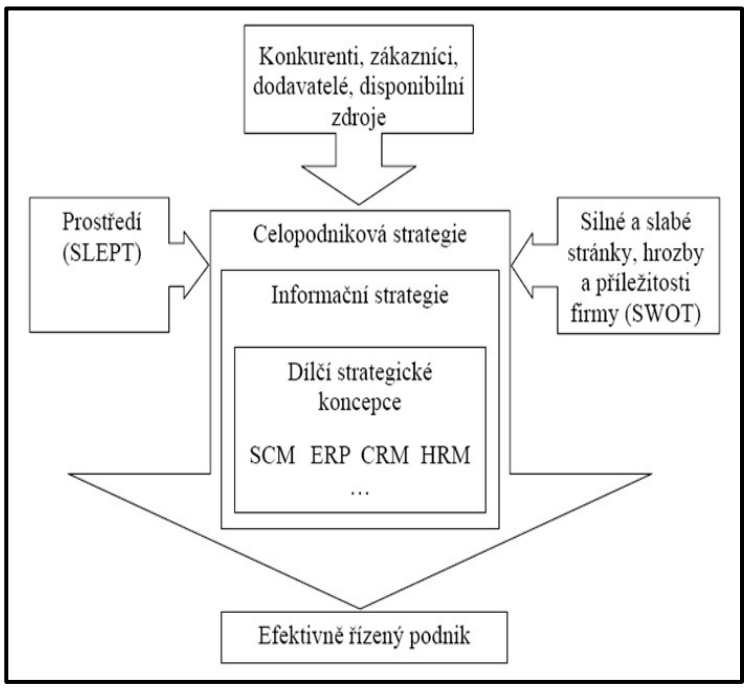
2.18. Informační strategie

Cílem informační strategie je optimální podpora zejména strategických cílů organizace a procesů v organizaci probíhajících, pomocí informačních systémů, informačních technologií a komplexních informačních služeb (Vymětal, Diačiková, Váchová, 2006). Informační strategie popisuje, jak podnik využívá existující data ke zvýšení své konkurenceschopnosti. Jedná se o neustále se vyvíjející plán, který zahrnuje pět kroků: stanovení, přizpůsobení, řízení, obměňování a optimalizace. Pakliže jsou všechny kroky harmonické, může firma optimalizovat své procesy, zvýšit svou produktivitu a zlepšovat rozhodovací postupy. Informační strategie je součástí všech

podnikových úrovní, od vedení společnosti přes všechny zaměstnance až po zákazníky a obchodní partnery (Informationsstrategie in fünf Schritten, 2011).

Globalizace, zvyšující se vzájemná závislost a vysoké riziko vedou ve spojení s explozivním nárůstem množství dat k neefektivnosti a stále větší komplexitě. Firmy se nacházejí v pozici, kdy se musejí rozhodovat co možná nejrychleji na základě jimi vybraných relevantních informací. IBM vytvořila na základě *Business Analytics and Optimization*[7] -optimalizačních řešení efektivní a účinnou informační strategii, která je výchozím bodem pro rozhodování, analýzu informací a tvorbu prognóz (Eine effektive Informationsstrategie dank Business Analytics and Optimization, 2010).

Následující schéma zobrazuje provázanost celopodnikové a informační strategie, které nemohou být tvořeny odděleně, naopak informační strategie musí navazovat na podnikatelskou a komplexní strategii řízení.



Obrázek 2-7 Vztah podnikové a informační strategie

Zdroj: IT Solution

Informační strategie je základním řízením strategického řízení podniku a je nezbytná pro plánování jeho rozvoje. Pro management společnosti je nástrojem k řízení informačních a komunikačních technologií. Tím je podnik schopen reagovat na potenciální

[7] Algoritmy a vysoce vyvinuté matematické zdroje, metody a funkce, které napomáhají k vytvoření analýzy předpokládaného vývoje, prognóz a podnikové optimalizaci (Business Analytics and Optimization, 2012).

útoky, jelikož má zabezpečení systémově zpracováno a riziko spojené s informačními hrozbami je eliminováno.

Jednotlivé kroky při tvorbě informační strategie jsou popsány v níže zobrazené tabulce.

	Efektivita	**Efektivita**
Potřeba rozhodnutí	Určení problému = Definování cílových kritérií	Realizace= Optimalizace Input/Output
Potřeba informací	Stanovení otázek = Definování informačního deficitu	Odpověď = Výběr informační strategie

Tabulka 2-3 Tvorba informační strategie

Zdroj: McLachlan in Ohliger

Prvotní krok k tvorbě informační strategie je existence informačního deficitu, který subjekt vnímá jako problém. Předtím než jsou stanoveny kanály pro vyhledávání informací, je nezbytné si určit kritéria k dosažení cíle a význam potřeby těchto informací, což slouží ke správné formulaci otázek. Následně jsou porovnávány nejrůznější možnosti k získávání dat, jejichž hlavním kritériem je efektivita. S tímto krokem úzce souvisejí náklady na zajištění požadovaných informací, které označujeme jako input, a následně analyzujeme efektivitu s reálným výstupem v podobě relevantních dat (McLachlan in Ohliger, 2005).

Informační strategie organizace je strukturována do čtyř oblastí (Vymětal, Diačiková, Váchová, 2006):

- Podnikatelská strategie - PROČ?
- Informační management - KDO, KDE, KDY?
- Informační systém - CO?
- Informační technologie - JAK?

Většina podniků disponuje podnikatelskou strategií, stejně tak IS a IT. Informační management je ale poměrně často tvořen separátně (vedení a IT oddělení), kdy mnohdy chybí potřebná komunikace a spolupráce. Dle Krcmare (2005) by měl informační management zastávat řídící úkoly týkající se IT vedení, strategie, IT procesů, IT zaměstnanců a IT controllingu. Model je dále rozčleněn do 3 podkategorií:

- Management informační ekonomiky (nabídka, poptávka, využití)
- Management informačních systémů (data, procesy, použití životního cyklu)
- Management informačních a komunikačních technik (ukládání, přepracovávání, komunikace, technické požadavky)

Dle autorů Vymětal a kol. by měla informační strategie obsahovat určité základní oblasti:

- Specifikace klíčových informací (pro hodnocení stavu trhu, pro vyhodnocování trendů vývoje trhu, o postavení organizace na trhu s ohledem na konkurenci, pro vyhodnocení aktuálního interního stavu organizace).
- Přehled standardů, které chce organizace uplatňovat při budování informačního systému.
- Objem finančních prostředků a dalších zdrojů, které organizace vyčlení na realizace informační strategie.
- Program rozvoje informačního systému ve střednědobém a dlouhodobém horizontu.

Ve společnostech obecně je kladen větší důraz na informační technologie a systémy, ale bývá opomíjen význam relevantních informací, které se stávají konkurenční výhodou. Problémem je také nedostačující investice do vzdělávání a proškolování zaměstnanců v této oblasti, jelikož lidský faktor je právě tím největším rizikem.

Plánování a efektivita jsou pro správné fungování informační strategie směrodatnými aspekty, na druhou stranu je velmi složité měřit úspěšnost a výsledky plynoucí z integrování této strategie do podnikové kultury. Mezi základní překážky patří nemožnost vyhodnocení výsledků za určité fixní období, jelikož tyto se mohou projevit až během budoucích let, další skupinu tvoří aspekty alokační – tzn. alokace nákladů, výhod, zaměstnanců, produktů atd. Dále se jedná o aspekt vývojový, kdy výsledky a změny

plynoucí z informační strategie lze stanovit pouze metodou ex post a to pomocí historických dokumentů a interview, což může být ovlivněno určitou dávkou subjektivity. A jako poslední je uváděn faktor rámcový, kdy výsledky z informační strategie mohou nabírat různých pohledů z hlediska jejího dopadu do různých podnikových oblastí a to vliv na vývoj IS, změny v podnikové strategii, kvalita IS a další (Galliers, Leidner, 2003).

Je podstatné zdůraznit, že tvorba informační strategie je pro každou organizaci individuální činností, která může vycházet pouze z určitých obecných koncepcí, ale v konečném důsledku je přizpůsobována přesně potřebám daného podniku.

2.19. Podceňování hrozeb

Výzkum společnosti Symantec byl realizován telefonicky v září 2011. Zúčastnilo se ho 1 900 organizací z celého světa. Jedna čtvrtina respondentů spadala do kategorie firem s 5 až 49 zaměstnanci, druhá měla 50 až 99 pracovníků, třetí čtvrtina zaměstnávala 100 až 249 lidí a poslední 250 až 499 osob. Dotazováni byli pracovníci, kteří spravovali výpočetní zdroje (Malé a střední firmy podceňují hrozbu cílených kyberútoků).

Hlavní zjištění výzkumu:

- **Malé a střední podniky ví o bezpečnostních rizicích**

Více než polovina malých a středních podniků je obeznámena s mnoha různými bezpečnostními hrozbami, jako jsou cílené útoky, zaznamenávání stisku kláves nebo hrozby plynoucí z užívání chytrých mobilních telefonů. Více než polovina respondentů (54 %) uvedla, že škodlivé kódy mohou vést ke ztrátě produktivity. 36 % pokládá možnost přístupu hackerů ke chráněným informacím za pravděpodobnou. 46 % dotázaných uvedlo, že cílený útok by měl za následek výpadek tržeb a dle názoru 20 % by odvedl zákazníky.

- **Malé a střední podniky se nepovažují za cíle**

Ačkoli podniky ví o nebezpečí kybernetických útoků, nemají pocit nebezpečí. Polovina malých a středních podniků se domnívá, že je chrání jejich velikost. Útoků by se podle nich měly obávat především velké organizace. Tento názor je v přímém rozporu se statistikami. Podle údajů ze sítě Symantec.cloud bylo vloni 40 % cílených útoků vedeno proti společnostem s nejvýše 500 zaměstnanci. Na korporace se přitom zaměřilo jen 28 % napadení.

- **Podniky se nevěnují prevenci**

Protože se malé a střední podniky nepovažují za cíle útoků, mnoho z nich selhává při zavádění základních opatření na ochranu informací. Zatímco dvě třetiny podniků sledují a omezují počet lidí s přihlašovacími údaji, 63 % vůbec nezabezpečuje počítače, které jsou využívány pro elektronické bankovnictví. 61 % dotázaných nemá nainstalován antivirový program na všech počítačích, 47 % nechrání své emailové servery nebo služby.

3 CHARAKTERISTIKA ZEMĚDĚLSKÉHO PODNIKU

3.1. Analyzovaná společnost

Společnost LUKROM, spol. s r.o., vznikla v roce 1991. Zpočátku představovala společnost, která byla zaměřena výhradně na obchodování se zemědělskými komoditami. Během svého vývoje se postupně vyvinula ve společnost zabezpečující komplexní služby zemědělské veřejnosti. Zakladatelem a současně majitelem podniků skupiny LUKROM je Zdeněk Červenka.

Společnost LUKROM, spol. s r.o., je tvořena šesti divizemi. Tzv. rostlinnou vertikálu tvoří divize agrochemie a divize zemědělských komodit, které se soustředí na poskytování služeb v rostlinné výrobě. Živočišná vertikála se skládá z divize výroby krmných směsí a divize živočišné výroby, které se zaměřují na služby pro živočišnou výrobu. V roce 2009 zanikla fúzí společnost Lukrom Zlín a.s. a její činnost byla začleněna do struktury společnosti LUKROM, spol. s r.o., jako divize zemědělské techniky. Divize ekonomicko-právní zabezpečuje chod společnosti z hlediska účetních, ekonomických, finančních a právních záležitostí.

LUKROM, spol. s r.o., za dobu svého působení vytvořila nebo kapitálově vstoupila do společností, které se zabývají zemědělskou prvovýrobou nebo poskytují služby na agrárním trhu. Prostřednictvím těchto aktivit je postupně vytvářena skupina LUKROM.

Analýza zkoumané problematiky probíhala jak napříč divizemi v mateřské firmě, tak také v rámci vybraných dceřiných společností patřících do holdingového seskupení. Podrobnější struktura je zobrazena v oddíle 3.3. Organizační struktura.

3.2. Vývoj společnosti

V následující tabulce jsou zachyceny zásadní milníky ve vývoji podniku od jeho založení až po současnost.

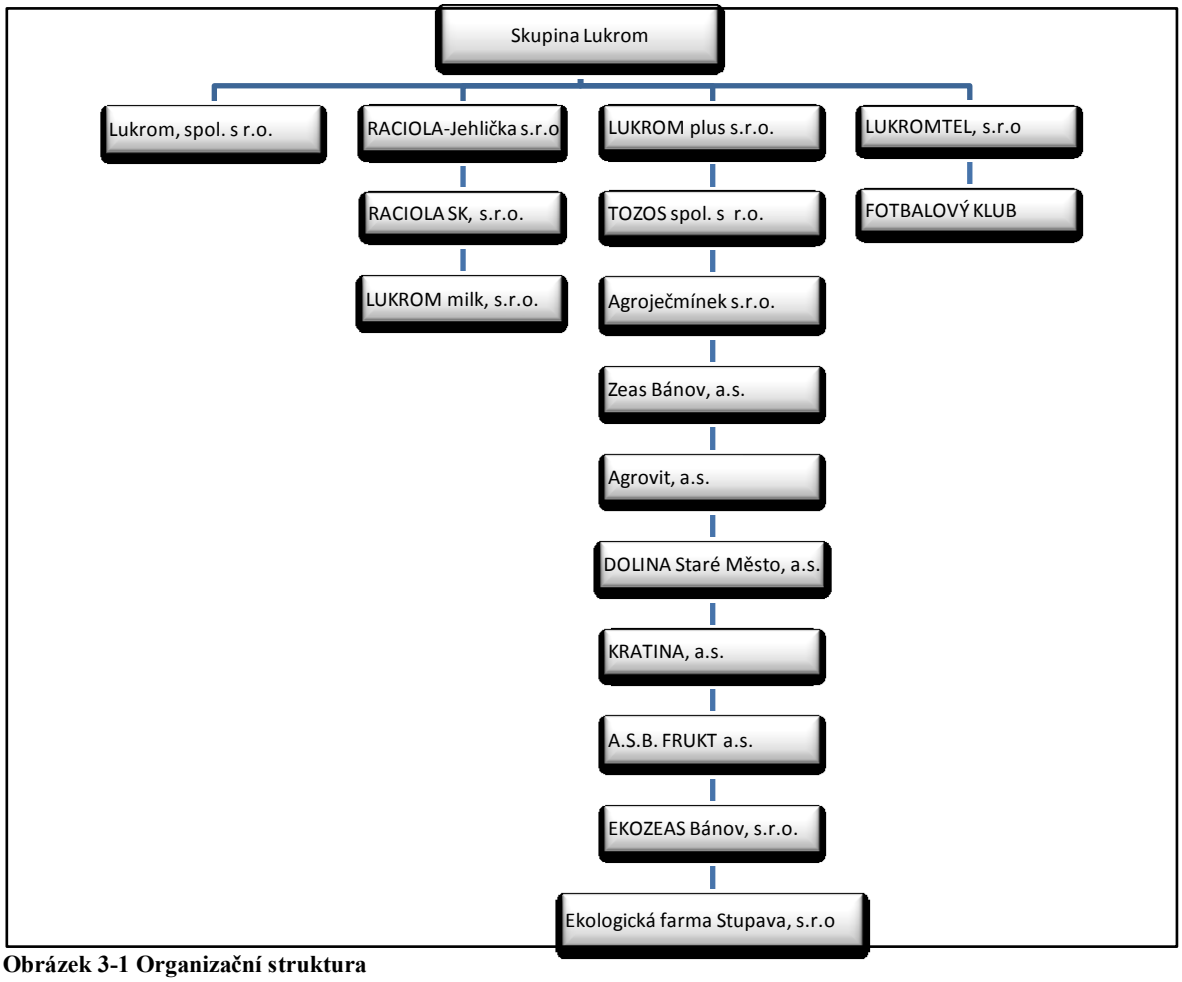
1991	Založení LUKROM, spol.s r.o.
1991	Vznik samostatných středisek prodeje strojů pro zemědělství, výrobu krmných směsí, prodeje agrochemikálií, živočišné a potravinářské výroby.
1993	Specializace na velkovýrobu, začátek realizace koncepce „zeleného úvěru“. Rozšíření sortimentu nabízených strojů, např. o značku John Deere.
1996	Vznik dceřiné společnosti LUKROM plus s.r.o. zabývající se rostlinnou prvovýrobou, hospodařící na 5 806 ha zemědělské půdy v regionech Jarohněvic, Tlumačova, Halenkovic, Bánova, Hustopečí nad Bečvou a Boršic u Buchlovic.
2000	Osamostatnění Lukrom Zlín a.s. za účelem zkvalitnění prodeje a servisu zemědělské techniky, náhradních dílů a veškerých ostatních služeb souvisejících s výhradním zastoupením zahraničních firem na českém a slovenském trhu. Koupě prvoligového fotbalového klubu FC TESCOMA Zlín, a.s.
2001	Vznik druhé dceřiné společnosti LUKROMTEL, s.r.o. V historii skupiny LUKROM se jako vůbec první samostatný podnikatelský subjekt nezabývá zemědělskou činností. Specializuje se na výstavbu základnových stanic, telekomunikačních a datových sítí, jejich servis a údržbu.
2002	Nákup společnosti Agroječmínek, s.r.o. v Chropyni, která se zabývá chovem skotu a produkcí mléka. Raritou je největší koncentrace krav o cca 1100 kusech.
2003	Nákup společností: • ZEAS Bánov, a.s. – chov skotu a výroba mléka • Agrovit, a.s. se sídlem ve Svatobořicích - Mistříně – rostlinná prvovýroba, porodna a výkrm prasat • DOLINA Staré Město, a.s. – rostlinná prvovýroba včetně produkce osiv, • otevření pneuservisu v nově zrekonstruované budově Lukrom Zlín a.s. v Kroměříži
2004	Vznik společnosti EKOZEAS Bánov, s.r.o. s ekologickou zemědělskou prvovýrobou.
2005	Založení společnosti LUKROM milk, s.r.o., která dodává dojírenské technologie včetně náhradních dílů. Rozšíření činnosti Lukrom Zlín a.s. o středisko mechanizace v Hulíně, které nabízí kompletní dodávky rekonstrukce a stavby dojíren, montáž všech typů dojírenské technologie včetně programového vybavení.
	Odkup konkurzní podstaty společnosti Agrosovín a.s., čímž se součástí skupiny stávají: • vinný sklep Sovín – vinné hospodářství a 110 ha vinic • A.S.B. FRUKT Buchlovice – ovocné sady • LIKOD, s.r.o. – těžba štěrkopísku

2006	• Ekologická farma Stupava, s.r.o. – ekologická zemědělská výroba
2007	Kapitálový vstup do společnosti RACIOLA-JEHLIČKA s.r.o. a RACIOLA SK, s.r.o. zabývající se porážkou drůbeže, zpracováním a prodejem drůbežích výrobků. Odkup majoritního podílu společnosti KRATINA, a.s. v Dolních Bojanovicích, činností podniku je chov skotu a rostlinná výroba včetně produkce zeleniny.
2009	Prodej společnosti LIKOD, s.r.o. Pronájem vinného sklepa Sovín, ukončení činnosti zpracování vína. Navýšení základního kapitálu v obchodní společnosti Raciola - Jehlička, s.r.o. na 82,3%. Zánik společnosti Lukrom Zlín a.s. fúzí se společností LUKROM, spol. s r.o., a začlenění její činnosti do organizační struktury LUKROM, spol. s r.o. jako divize zemědělské techniky.
2010	Prodej vinic. Nákup 60% podílu ve společnosti TOZOS spol. s r.o.
2011	V rámci konsolidace holdingu LUKROM došlo v uplynulých měsících k navýšení majetkové účasti ve společnosti KRATINA, a.s. a DOLINA Staré Město, a.s.

Tabulka 3-1 Vývoj společnosti

Zdroj: LUKROM

3.3. Organizační struktura



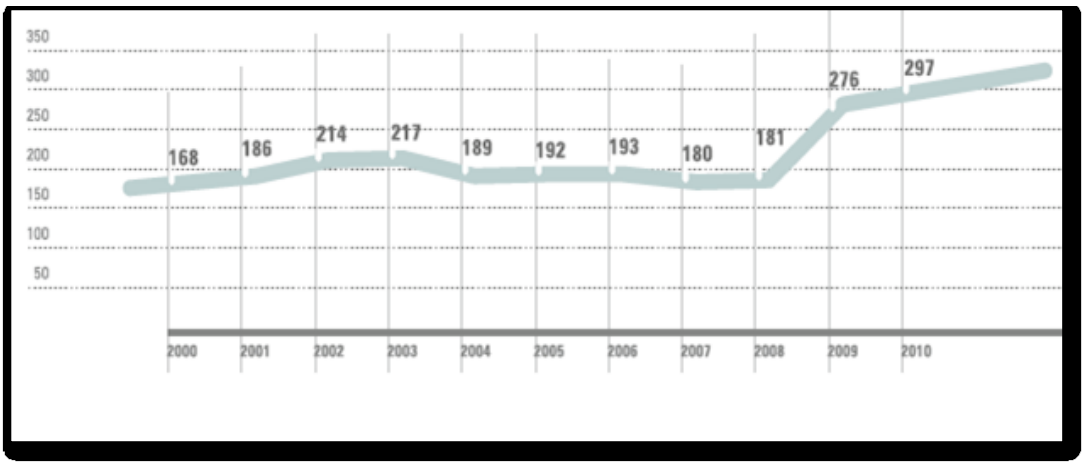
Obrázek 3-1 Organizační struktura

Zdroj: LUKROM

Skupina Lukrom je tvořena poměrně velkým počtem podniků, které zaštiťuje LUKROM, spol. s r.o. Jejich pole působnosti se nezaměřuje pouze na oblast zemědělství, ale portfolio zahrnuje i např. fotbalový klub či telekomunikační a datové sítě.

3.4. Vývoj zaměstnanců a tržeb LUKROM, spol. s r.o.

Níže uvedené grafické zpracování údajů o vývoji počtu zaměstnanců a tržeb zachycuje změny obou hodnot v rozmezí jedné dekády, přičemž jednotlivé odchylky jsou zpracovány za období jednoho roku. Na horizontální ose jsou jednotky časové (rok), vertikální osa znázorňuje počet zaměstnanců.

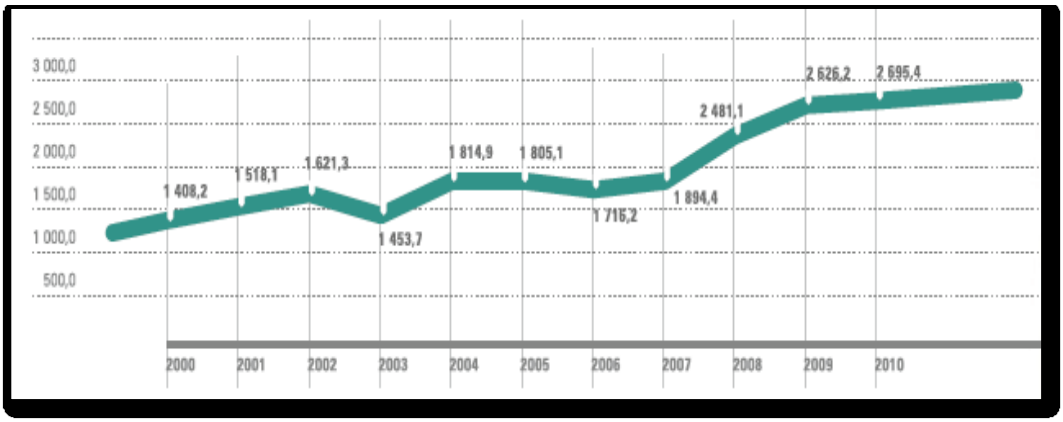


Graf 3-1 Vývoj počtu zaměstnanců (období 2000 – 2010)
Zdroj: LUKROM

Křivka od roku 2000 až po začátek roku 2008 je poměrně stálá, s horizontálním charakterem vývoje, a bez větších výkyvů. Průměrný počet zaměstnanců je 191. Rostoucí trend je zřetelně vykazován v letech 2008 až 2010. Za poslední měřitelné období je stav zaměstnanců 297.

I přes nepříznivé podmínky, které vyvolala celosvětová krize, se podnik nedostal do fáze snižování stavu zaměstnanců, naopak navzdory trendu propouštění zvyšoval počty svých pracovníků.

Vzhledem k problematice informační bezpečnosti je společnost s vysokým počtem zaměstnanců náchylnější k možným útokům a ztrátě dat a informací. Směrodatné je mít zpracovaný dokument, který se zabývá právě interní a externí bezpečností a ochrany informací a který je aplikovatelný na všechny jednotky ve skupině podniků jako je LUKROM. Podnik zaměstnává necelých 300 lidí, z nichž každý může být potenciální hrozbou pro podnik, ať již vědomě či nevědomě.



Graf 3-2 Vývoj tržeb (období 2000 – 2010)

Zdroj: LUKROM

Vývoj tržeb LUKROM, spol. s r.o., již není tak kontinuální jako v případě vývoje počtu zaměstnanců. Přesto i s jediným větším propadem v 2003 můžeme zaznamenat rostoucí trend, který nabývá svého maxima právě v roce 2010. Výroční zpráva za rok 2010 hodnotí ekonomickou situaci podniku trvale příznivě a stabilně – signalizuje posílení ekonomické situace společnosti (Holeček, 2010).

Pozitivní vývoj tržeb a celkové situace v podniku by mělo být také přímo úměrné s investicemi do vzdělávání zaměstnanců o informačních hrozbách a jejich předcházení. Vzhledem k úspěšnosti firmy a příznivým vyhlídkám i do budoucnosti se teoreticky může dostat do střetu s hackerskými útoky, kterým se v současné době nevyhýbají ani takovým jako je OSN, česká či slovenská vláda. LUKROM, spol. s r.o., má významnou tržní pozici v regionu a patří k předním poskytovatelům komplexních služeb pro zemědělskou veřejnost.

4 ANALÝZA SOUČASNÉHO STAVU INFORMAČNÍ STRATEGIE

4.1. Specifikace předmětu analýzy

Analýza je zaměřena v obecné rovině na problematiku informační bezpečnosti podniku, která je dále rozpracovávána do konkrétní oblasti týkající se zaměstnaneckého povědomí o informačních hrozbách a jejich předcházení, rozdělení kompetencí a odpovědnosti za informační bezpečnost a v neposlední řadě potřeby interního dokumentu upravující ochranu dat a informací. Veškeré získané údaje z uvedených oblastí se stávají stěžejním bodem pro určení směru informační strategie podniku, která musí být zcela kompatibilní s analyzovanou společností a musí být přizpůsobena její specifické struktuře a systému.

Cílem analýzy je zajištění adekvátních informací, které umožní stanovit výrok o současném stavu informační bezpečnosti v podniku. Pro získání potřebných informací byla zvolena jedna metoda sběru dat – dotazníkové šetření, jehož výstup poté vede k verifikaci či falzifikaci původních domněnek. K bližší specifikaci cíle byly použity výzkumné otázky, které zpřesňují pohled na danou problematiku a vytváří konkrétní zaměření. Mezi stěžejní otázky analyzované problematiky patří:

- Je zabezpečení dat a informací v podniku na adekvátní úrovni?
- Disponují zaměstnanci dostatečnými informacemi o potenciálních hrozbách a jejich předcházení?
- Která podniková složka má hlavní odpovědnost v oblasti informační bezpečnosti?
- Existuje interní dokument zabývající se informační bezpečností?

Po definování výzkumných otázek navazuje fáze operacionalizace, jež vychází z hypotéz popisujících výzkumný problém. Dotazník je sestaven takovým způsobem, aby co nejlépe zmapoval konkrétní otázky informační bezpečnosti. Je zaměřen na teoretické a praktické znalosti zkoumané problematiky ze strany zaměstnanců, na jejich názory a postoje, jejich případné reakce v krizových situacích a další fakta.

Hypotézy, které slouží jako podklad k operacionalizaci, zní:

H1: *„Zaměstnanci nedisponují dostatečnými informacemi o potencionálních informačních hrozbách a jejich předcházení.“*

H2: *„Informační bezpečnost je výhradně v kompetencích IT oddělení.“*

H3: *„V podniku chybí zpracovaný dokument zabývající se informační bezpečností.“*

Vzhledem ke zvolené metodě získávání dat jsou náklady na výzkum zanedbatelné. Dotazník byl vytvořen odpovídajícím způsobem tak, aby mohl být použit k elektronickému vyplnění přes email. Tímto také odpadají náklady na tisk dokumentu a další náklady související s doručením dotazníků do vybrané společnosti jako cestovní výdaje. Nespornou výhodou je menší časová náročnost než v případě osobního kontaktu, na druhou stranu je zároveň i nevýhodou, pokud má zaměstnanec určité otázky. Volba emailové komunikace v této konkrétní situaci je nejlepší variantou, jelikož byla provedena pilotáž, aby došlo k eliminaci možných nesrovnalostí v dotazníku.

4.2. Postup analýzy a použité metody

4.2.1. Použité metody sběru dat

V závislosti na povaze zkoumané problematiky byla ke sběru dat aplikována pouze jedna metoda – dotazníkové šetření. Jelikož informační bezpečnost a z ní plynoucí strategie jsou záležitostí podniku jako celku, volba jednotného dotazníku je tou nejlepší možností k získání potřebných informací a jejich následné analýzy.

Koncepce jednotlivých tvrzení v dotazníku je uzpůsobena tak, aby bylo možné jeho plošné použití na zaměstnance, tzn. napříč celou organizační strukturou počínaje top managementem a konče u nejnižších pozic, kteří mohou být teoretickým zdrojem možného selhání v oblasti informační bezpečnosti. Dotazník je složen z jednotlivých tvrzení, popřípadě otevřených otázek, jejichž účelem je zmapování současné úrovně informačního povědomí u zaměstnanců. Možnosti odpovědí by měly pokrývat co nejširší pole působnosti, ve kterém není respondent omezován a je mu umožněn vyjádřit co nejobjektivnější názor. V případě postojových tvrzení byla použita pětistupňová tzv. Likertova stupnice.

Dotazníkové šetření bylo naplánováno uskutečnit pouze v elektronické formě s využitím emailové komunikace. Výhodou zvolené komunikace jsou minimální náklady na provedení výzkumu a úspora času. Dotazník byl proto k tomuto účelu přesně sestaven tak, aby respondenti byli schopni s minimálním úsilím jej vyplnit a zpětně odeslat. Každý ze zaměstnanců obdržel dotazník v emailové příloze s potřebnými instrukcemi k jeho správnému vyplnění nejen přímo v dotazníku, ale také v samotném emailu. Tímto krokem měla být eliminována neochota k jeho vyplnění a zajištěna maximální návratnost. Jednoznačnou nevýhodou elektronické komunikace je bezpochyby nemožnost osobního kontaktu a případná asistence při nepochopení otázky či jiných problémech. Aby došlo k co největšímu snížení tohoto handicapu, byla provedena pilotáž před rozesláním finální verze dotazníku.

Při zpracování dat byla využita kvalitativní metoda.

4.2.2. Výběr respondentů

Vzhledem ke zkoumané problematice, jež se týká všech zaměstnanců bez výjimky, byl výběr respondentů náhodný. Podstatou však bylo zajistit průřez všemi sférami organizační struktury a docílit tak vysoké vypovídací hodnoty nasbíraných dat. Plánovaný počet respondentů byl stanoven na 50, což bylo naplněno ze 74 %. 37 plnohodnotných dotazníků tak umožnilo podrobnější analýzu. Podstatným hlediskem, které ovlivnilo původní očekávání, byla forma elektronické komunikace, jež neumožňuje přímý kontakt s respondentem. Dalším faktorem byla také nemožnost v některých případech využít dotazníky k dalšímu zpracování z důvodu jejich chybného či nedostatečného obsahu.

Výzkum byl proveden nejen v mateřské společnosti LUKROM, spol. s r.o., ale také v dceřiných podnicích RACIOLA – Jehlička s. r. o. a LUKROM plus s. r. o. Povaha zkoumané oblasti dovolovala zapojit širokou škálu respondentů a tím zvyšuje šance na co nejméně zkreslené výsledky šetření, které by mohly nastat v případě, že zaměření by bylo pouze na IT oddělení a vrcholový management, kteří disponují větším objemem informací.

4.2.3. Pilotáž

Součástí analýzy byla také pilotáž neboli předvýzkum. Tato část pomohla odbourat nepřesnosti ve struktuře a obsahu dotazníku. Došlo k ověření, zda jednotlivá tvrzení jsou pro tázané jednoznačná a srozumitelná. Zda jsou odpovědi správně naformulované s dostatečnou škálou pro výběr. Jestli dotazník není sugestivní a nenavádí přímo k určité odpovědi. Důležitým faktorem byla také časová náročnost na vyplnění a konstrukce dotazníku s ohledem na volbu elektronické formy komunikace se zaměstnanci. Díky pilotáži došlo k redukci možných chyb, nesrovnalostí a neochoty k účasti.

4.3. Výsledky analýzy

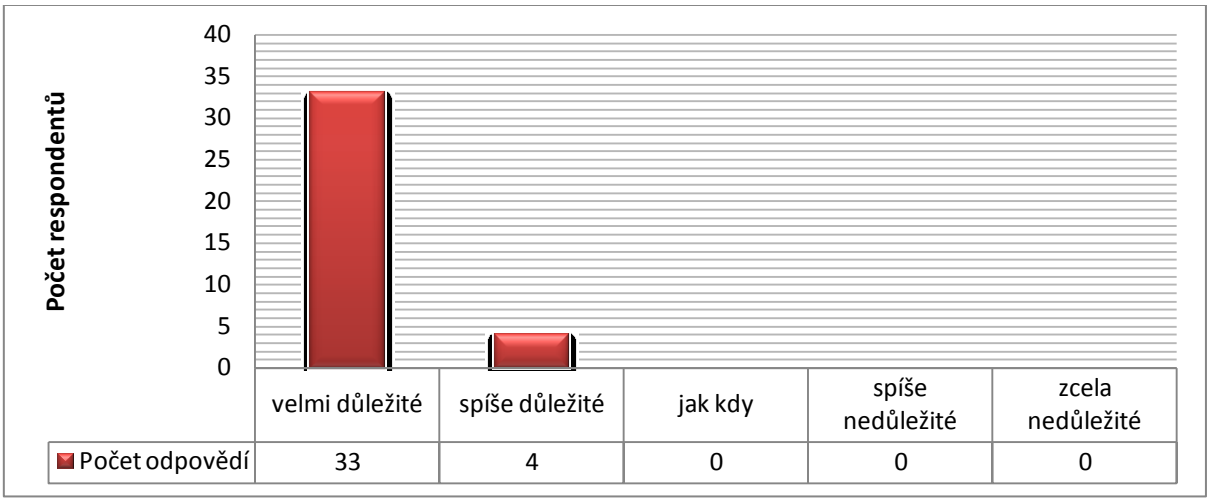
K analýze byla využita pouze jedna metoda – dotazníkové šetření. Volba emailové formy komunikace byla zvolena z důvodů časových a vzhledem k nákladům v případě osobního kontaktu s respondenty.

Výsledky jsou prezentovány v jednotlivých grafických zpracováních, vždy doplněny o komentář k danému tvrzení.

4.3.1. Popis a interpretace dílčích zjištění

Význam informací a jejich bezpečnost pro podnik

Význam informací a jejich bezpečnost pro podnik byl zjišťován pomocí dotazníkového tvrzení č. 1 (Význam informací a jejich bezpečnost jsou pro podnik). Výsledná zjištění jsou uvedena v grafu č. 4-1.



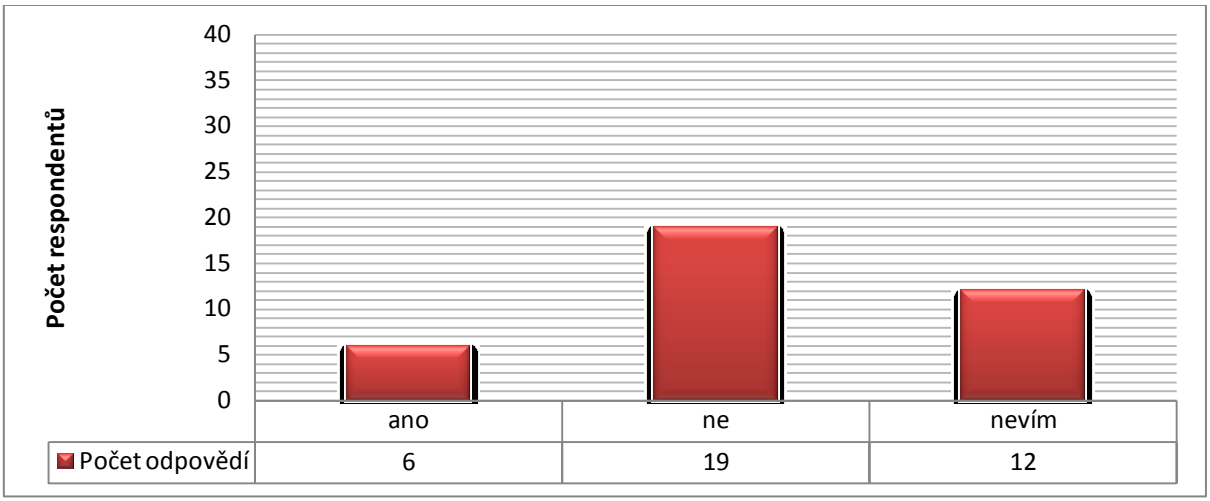
Graf 4-1 Význam informací a jejich bezpečnost pro podnik

Zdroj: Vlastní

V grafu jednoznačně dominuje odpověď *velmi důležité* (89 %), což je důkazem toho, že dotazovaní si uvědomují význam podnikových informací a jejich bezpečnost. Malé procento odpovědí poté zaujímá ještě možnost *spíše důležité* (11 %). Ostatní varianty nebyly respondenty zvoleny vůbec. Postoj ve firmě k ochraně dat a informací je jednoznačně pozitivního charakteru. Zde se však nacházíme pouze v teoretické rovině pohledu na danou problematiku.

Podniková školení týkající se informační bezpečnosti

Zda jsou prováděna školení v oblasti informační bezpečnosti, bylo zjištěno pomocí dotazníkového tvrzení č. 2 (V podniku jsou prováděna školení týkající se informační bezpečnosti), kdy jeho součástí bylo i několik příkladů pro snížení potenciálního neporozumění otázce. Výsledná zjištění jsou uvedena v grafu č. 4-2.



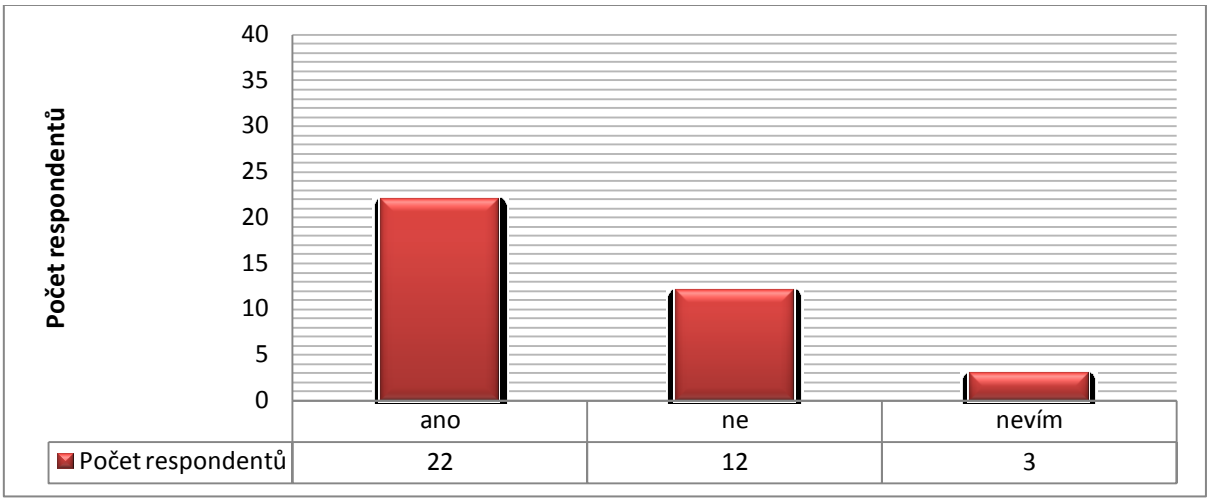
Graf 4-2 Podniková školení v informační bezpečnosti

Zdroj: Vlastní

V grafickém znázornění je viditelná nesourodost odpovědí, což naznačuje poměrně nejasnou situaci v podniku v oblasti školení. U menší skupiny zaměstnanců probíhá (16,2 %), většina respondentů (51,4 %) se ale domnívá, že taková školená vůbec neexistují, a o něco menší procento (32,4 %) z nich si není jisté. Z toho můžeme vyvodit, že firma se zaměřuje s největší pravděpodobností pouze na úzkou skupinu zaměstnanců, u nichž předpokládá nutnost vzdělávání v této oblasti.

Informační bezpečnostní incident

Tvrzení č. 3, které je opět doplněno o několik příkladů pro snadnější orientaci v problematice, (Setkali jste se již s nějakým informačním bezpečnostním incidentem) se zaměřuje na zkušenosti respondentů s jakýmkoliv bezpečnostním incidentem. Výsledná data jsou k dispozici v grafu č. 4-3.



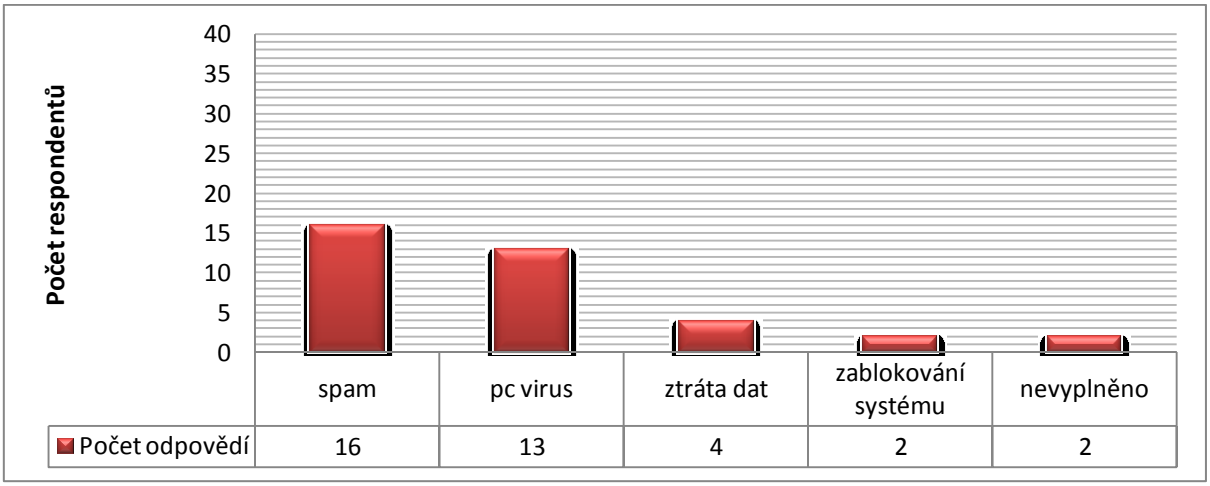
Graf 4-3 Zkušenosti s informačním bezpečnostním incidentem

Zdroj: Vlastní

60 % respondentů zvolilo odpověď *ano*, tedy že mají zkušenost s nějakým bezpečnostním incidentem, u něhož však neznáme míru závažnosti. 32 % označilo odpověď *ne*, což může být průvodním znakem toho, že tito zaměstnanci mají buď k dispozici dokonalejší ochranné technologie a znalosti, nebo výskyt těchto jevů neregistrují. 8 % odpovědí *nevím* potvrzuje neznalost možných informačních hrozeb.

Druh bezpečnostního incidentu

Tvrzení v pořadí č. 4 (Uveďte, prosím, druh bezpečnostního incidentu) navazuje na předchozí a slouží k přesnému určení druhu bezpečnostního incidentu. Spadá do kategorie otevřených otázek, kdy respondent nemá na výběr z několika možností, ale odpovídá samostatně. Výsledky jsou zpracovány v grafu č. 4-4.



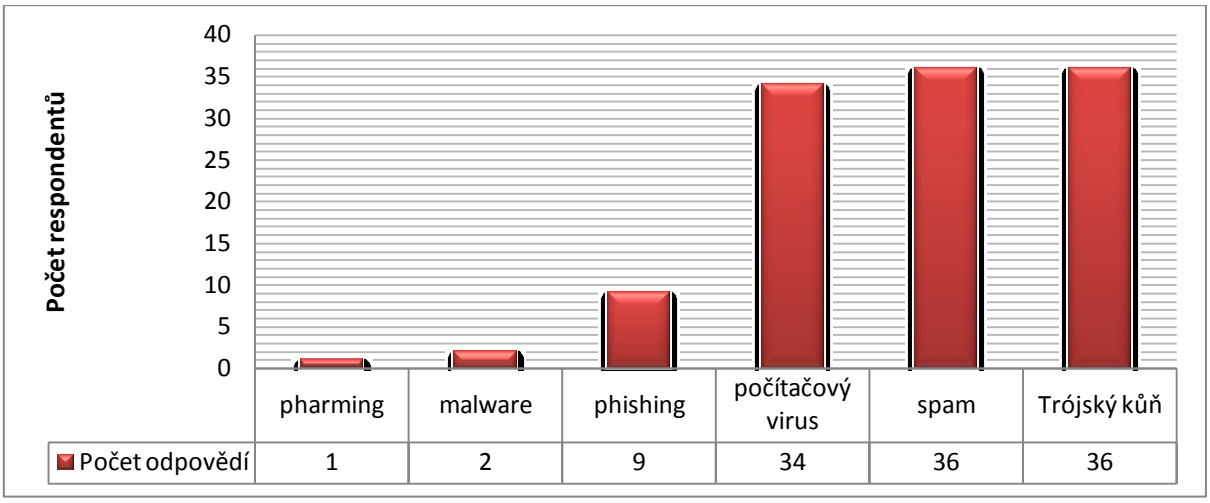
Graf 4-4 Druh bezpečnostního incidentu

Zdroj: Vlastní

Odpověď s největším výskytem byla *spam*, což ale není považováno za velké nebezpečí pro firmu. Dalším incidentem, se kterým se zaměstnanci setkali, byl *počítačový virus*, který již může být hrozbou. Zmíněny byly také *ztráta dat* a *zablokování systému*. Oba pojmy se mohou stát klíčové, pokud by se jednalo například o ztrátu citlivých dat, anebo pokud by původcem zablokování systému byl externí faktor – například hacker. Dva respondenti otázku nevyplnili, pravděpodobně z důvodu neznalosti názvu daného incidentu. Z celkového počtu 37 dotazovaných pak 14 odpovědělo v předchozí otázce NE nebo NEVÍM, a těch se tedy tvrzení č. 4 netýkalo.

Teoretické či praktické znalosti vybraných pojmů

Cílem tvrzení č. 5 (Které z následujících pojmů jsou pro Vás známé) bylo zjistit, do jaké míry jsou zvolené pojmy týkající se informačního ohrožení respondentům známé či nikoliv. Na základě zpracovaných údajů o nejčastějším výskytu škodlivých incidentů dle *CSIRT.CZ* bylo stanoveno šest možností: phishing, pharming, spam, malware, Trojský kůň a počítačový virus. Výsledná zjištění jsou uvedena v grafu č. 4-5.



Graf 4-5 Teoretické či praktické znalosti uvedených pojmů

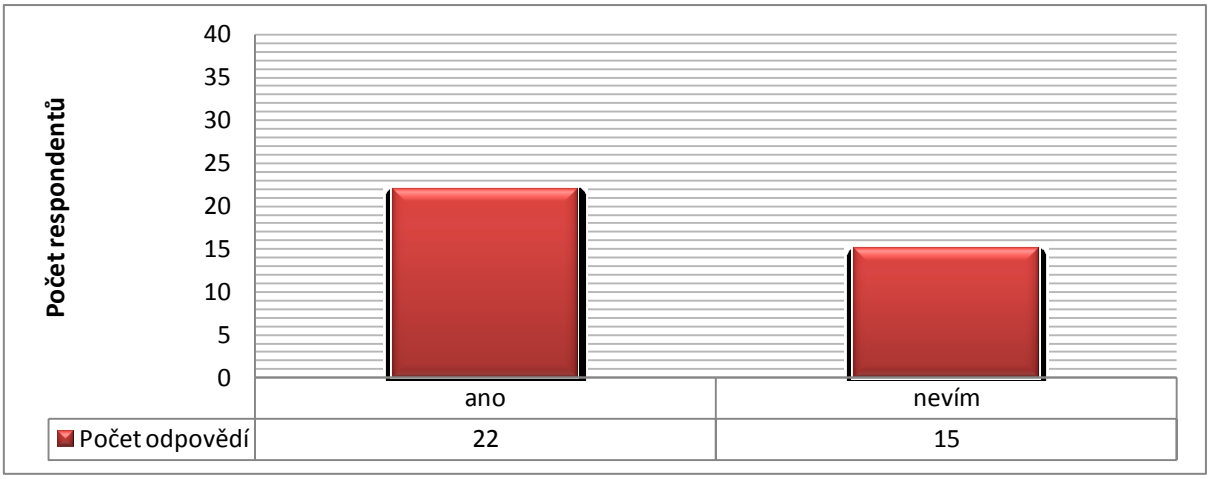
Zdroj: Vlastní

Z grafického zobrazení jednoznačně vyplývá převaha třech pojmů a to: *počítačový virus*, *spam* a *Trojský kůň*. Další v pořadí je *phishing* a nejméně početné odpovědi jsou *malware* a *pharming*. Pro každou firmu je pak rozhodující, jak pracovníci zareagují na vnější hrozby a jak aplikují své znalosti a zkušenosti na vyskytující se jev. V prvé řadě musí být zajištěna ochrana v podobě antivirových programů a dalších softwarových

aplikací, v druhé řadě musí být zaměstnanci obeznámeni s možnými riziky a musí vědět, jak v dané situaci dále postupovat.

Úroveň bezpečnosti informací a informačního systému

Názor na současný stav bezpečnosti informací a informačního systému bylo zjišťováno pomocí tvrzení č. 6 (Je dle Vás v podniku zajištěna bezpečnost informací a informačního systému na dostatečné úrovni). Výsledky jsou prezentovány v grafu č. 4-6.



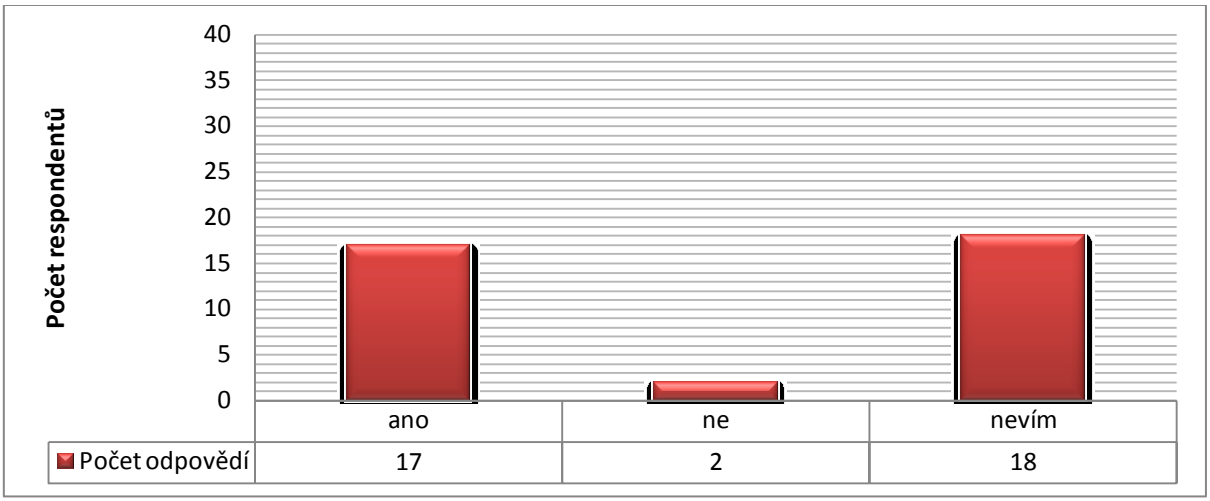
Graf 4-6 Úroveň bezpečnosti informací a informačního systému v podniku

Zdroj: Vlastní

V grafu jsou zastoupeny pouze dvě ze tří možných odpovědí. Větší polovina respondentů je se současným stavem spokojena. Zbývající část označila odpověď *nevím*, což naznačuje existenci možných nedostatků. Směrodatné však zůstává, jestli se jedná pouze o drobné mezery v zabezpečení informací a celkového informačního systému, nebo jde o větší nedostatky, které mohou firmu a její fungování ohrozit.

Podpora vedení v rámci ochrany a zabezpečení informací

Hlavním smyslem tvrzení č. 7 (Je dle Vašeho názoru zajištěna dostačující podpora vedení v rámci zabezpečení a ochrany informací) bylo objasnění postoje vedení společnosti k dané problematice a to napříč všemi stupni organizační struktury. Zjištěné výsledky jsou zobrazeny v grafu č. 4-7.



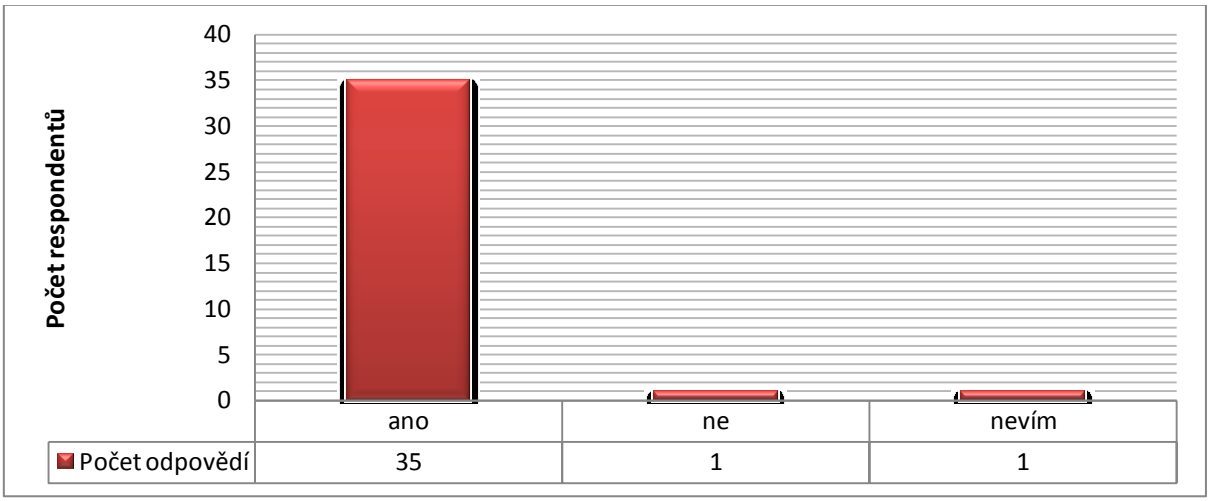
Graf 4-7 Podpora vedení společnosti k ochraně a zabezpečení informací

Zdroj: Vlastní

Z celkového počtu dotazovaných necelých 50 % se ztotožňuje s tvrzením, že podpora informační bezpečnosti v podniku je na dostatečné úrovni. Jako kontra argument je výsledek druhé poloviny respondentů, kteří se přiklání k odpovědi *nevím*, z čehož lze vyvodit, že management s největší pravděpodobností podporuje bezpečnost dat a informací na adekvátní úrovni, ale tyto informace se nedostávají na nižší organizační stupně. Pouze dva respondenti zastávají názor, že činnost ze strany vedení není dostačující.

Přístup k internetu

Úkolem tvrzení č. 8 (Máte k dispozici neomezený přístup k internetu) bylo stanovit podíl respondentů, kteří mají přístup k internetu, a tím definovat potenciální nebezpečí z lidského pochybení či neznalosti. Výsledná zjištění jsou v následujícím grafu č. 4-8.



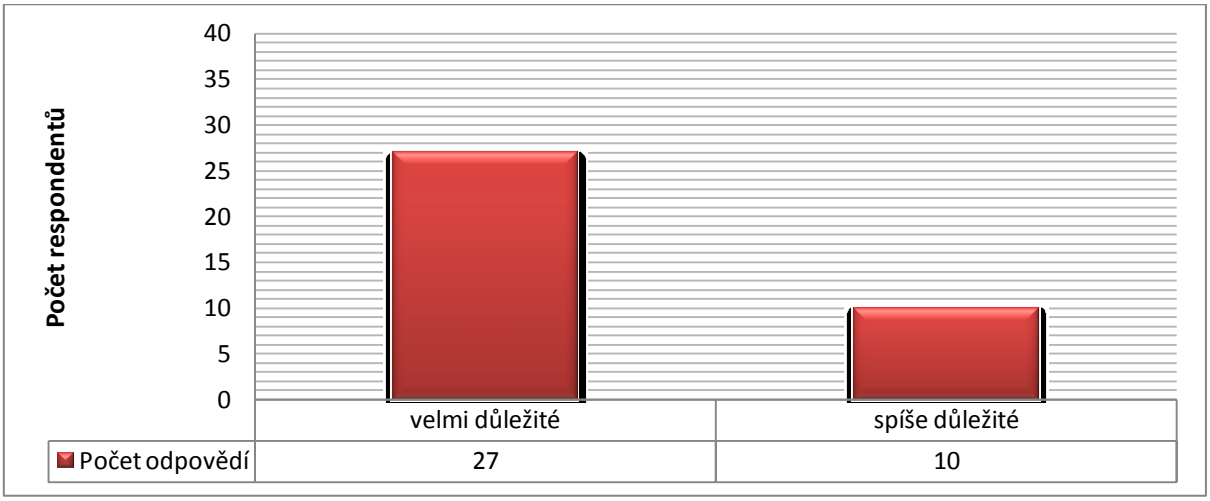
Graf 4-8 Přístup k internetu

Zdroj: Vlastní

Z grafického znázornění jednoznačně vyplývá, že téměř všichni respondenti mají k dispozici přístup k internetu (94,6 %). Odpovědi *ne* a *nevím* byly označeny každá pouze jednou. Vzhledem poměrně velkému počtu zaměstnanců narůstá i riziko zneužití informací (úmyslně či neúmyslně) za podpory internetu. Pro podnik je směrodatné proškolit své zaměstnance na minimálně základní úrovni ohledně internetových hrozeb jako je phishing, pharming a jiné.

Význam bezpečného používání internetu pro podnik

Tvrzení č. 9 (Dle Vašeho názoru je bezpečné používání internetu pro podnik) zjišťuje, jakou váhu respondenti kladou na nebezpečí při používání internetu a to na podnik jako celek. Výsledky jsou k dispozici v následujícím grafickém zobrazení č. 4-9.



Graf 4-9 Význam bezpečného používání internetu

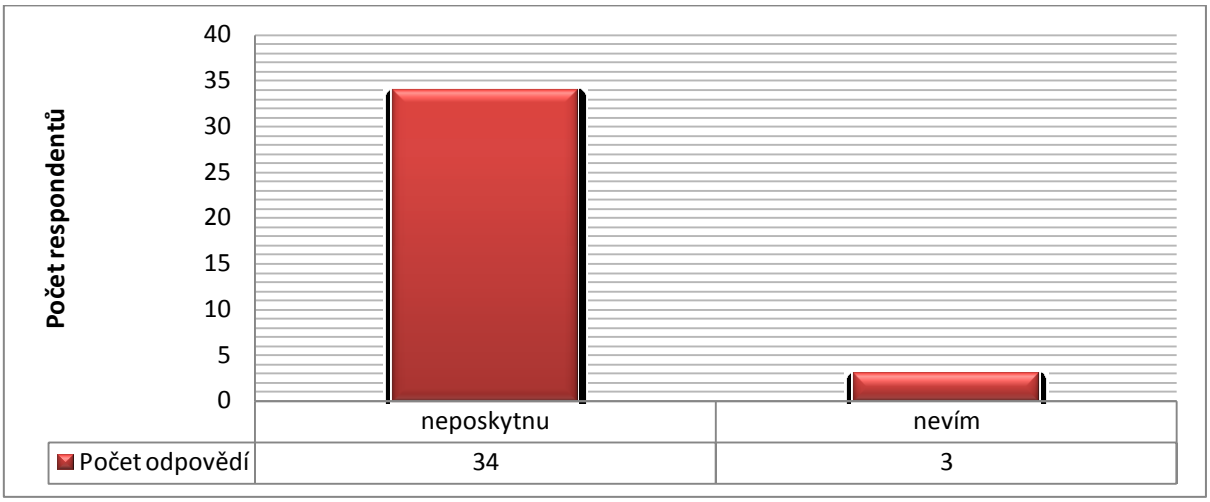
Zdroj: Vlastní

Z celkového počtu respondentů označilo odpověď *velmi důležité* 73 %, což vypovídá o uvědomování si potenciálních hrozeb. 27 % dotazovaných pak zvolilo možnost *spíše důležité*. Celkově můžeme zhodnotit výsledky tohoto tvrzení jako velmi uspokojivé, jelikož každý respondent si je vědom možných internetových útoků. Rozhodující je, jaká bude jeho reakce, pokud bude čelit skutečné hrozbě.

Poskytnutí informací osobě mimo podnik

Tvrzení č. 10 (V případě, že se dostanete do situace, kdy jsou po Vás žádány informace od osoby mimo podnik) patří mezi směrodatné pro podnik, jelikož odhaluje teoretické chování

zaměstnanců v situaci, kdy jsou po nich žádány interní informace společnosti. Výsledná zjištění jsou prezentována v následujícím grafickém zpracování č. 4-10.



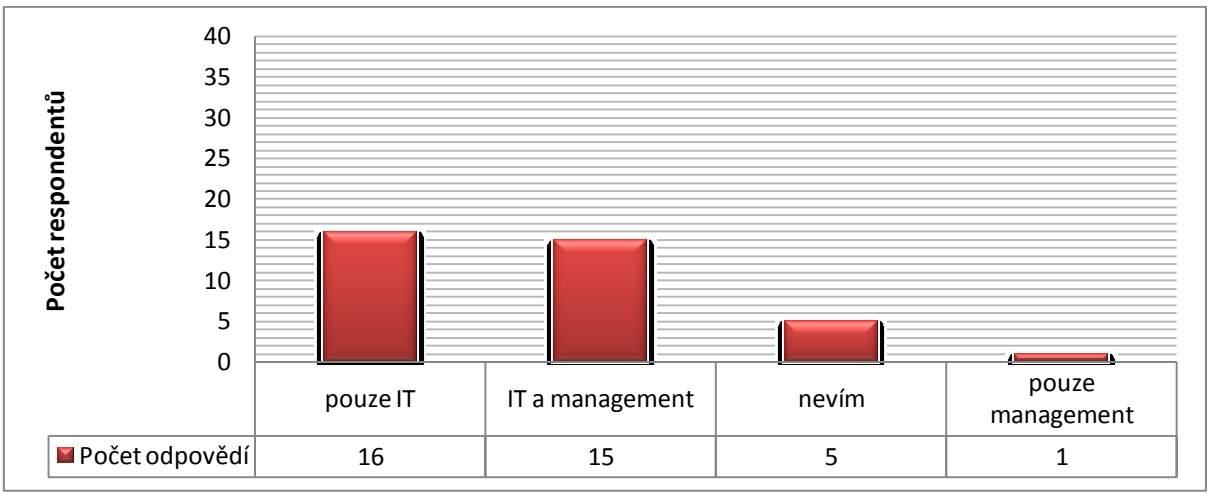
Graf 4-10 Poskytnutí informací osobě mimo podnik

Zdroj: Vlastní

Z grafu je patrné, že jednoznačnou převahu v odpovědích má možnost *neposkytnu* (92%) a jen nepatrné procento dotazovaných (8%) označilo variantu *nevím*. Podnik má tedy určité mezery, kde by měl svým zaměstnancům sdělit významnost informací a specifikovat hrozby, které následně firmě hrozí při úniku citlivých dat a informací.

Odpovědnost v podniku v oblasti ochrany informací

Tvrzení č. 11 (Kdo má v podniku odpovědnost za zajištění bezpečnosti v oblasti ochrany informací) pomáhá odhalit strukturu firmy a odpovědné osoby či oddělení za bezpečnost dat a informací. V grafu č. 4-11 jsou uvedena výsledná zjištění.



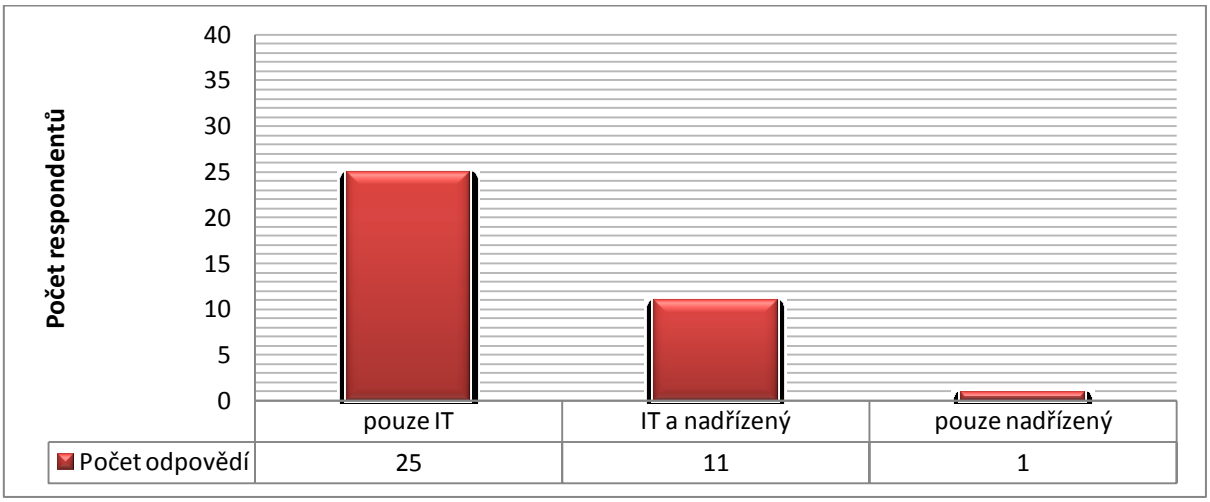
Graf 4-11 Odpovědnost za bezpečnost informací

Zdroj: Vlastní

V grafickém zobrazení je patrná určitá nesourodost odpovědí, což může být zapříčiněno neprůhledným systémem kompetencí nebo nedostatkem informací. 43,2 % zastává názor, že odpovědnost za bezpečnost podnikových informací má pouze IT oddělení. 40,5 % respondentů označilo možnost *IT oddělení a management*. 13,5 % neví, kdo má odpovědnost v této oblasti, a jen 2,7 % z celkového počtu odpovědí byla možnost *pouze management*.

Řešení závažného bezpečnostního incidentu

Tvrzení č. 12 (V případě závažného problému se obracím), které je doplněno o několik příkladů pro přesnou představu míněného problému jako např. ztráta informací či zablokování informačního systému, podává obraz o tom, jak by respondenti reagovali v dané situaci. Výsledná data jsou k dispozici v grafu č. 4-12.



Graf 4-12 Řešení závažného bezpečnostního incidentu

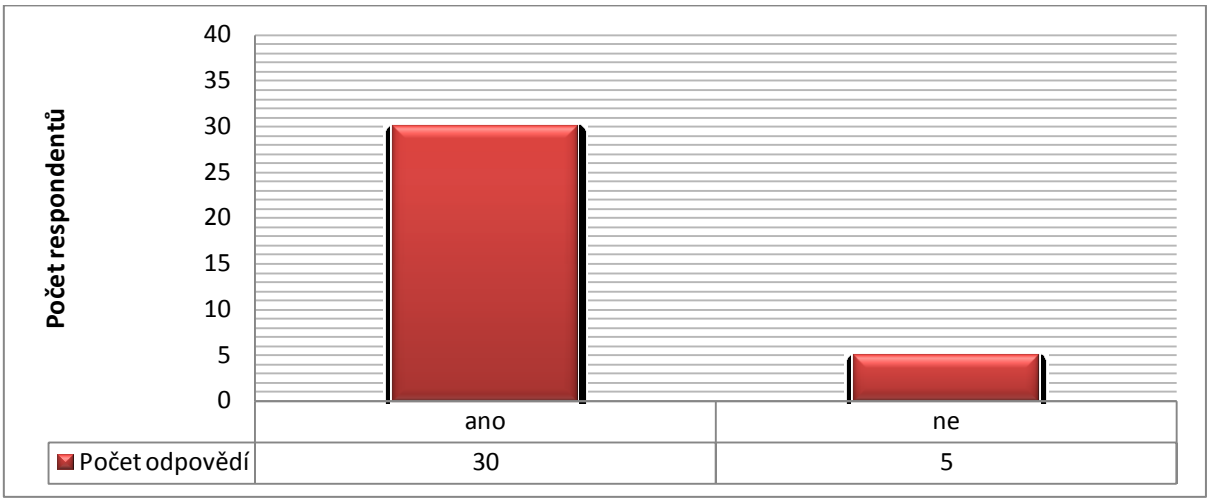
Zdroj: Vlastní

67,6 % respondentů by problém řešilo pouze s pracovníky IT oddělení. 29,7 % by se obrátilo jak na IT oddělení, tak i na svého nadřízeného. Pouze 2,7 % dotazovaných by využilo konzultaci pouze se svým nadřízeným. Pro podnik je podstatné, aby i management byl zapojen do dění v případě vysoké závažnosti informačního problému.

Úroveň vybavení podniku informačními technologiemi

Pomocí jednotlivých odpovědí respondentů na tvrzení č. 13 (Jsou dle Vašeho názoru informační technologie v podniku na adekvátní úrovni), jež bylo doplněno o příklady jako

počítačové vybavení, telefony či software, byly získány názory na úroveň vybavenosti podniku informačními technologiemi, které jsou zpracovány v grafu č. 4-13.



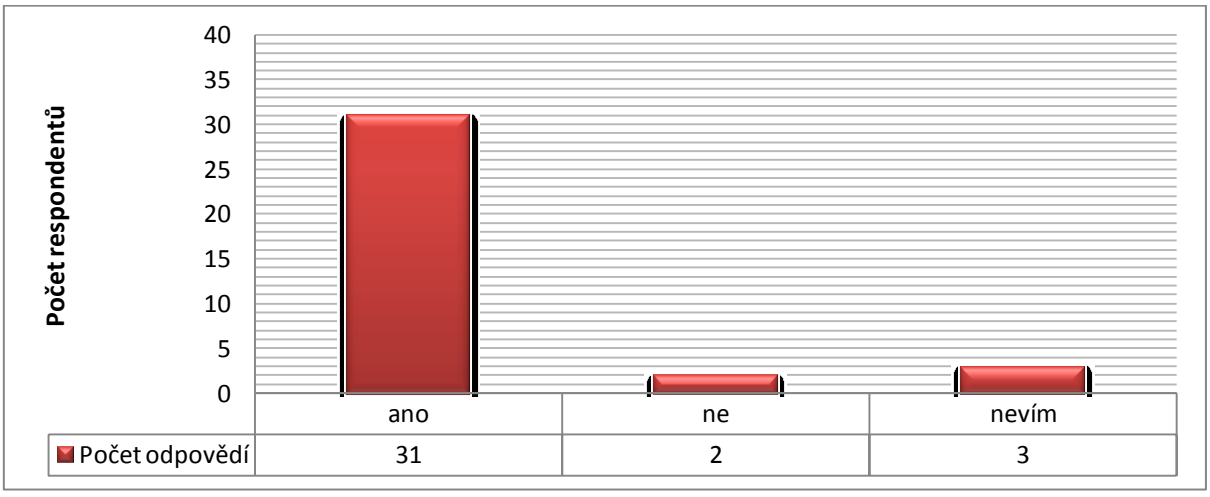
Graf 4-13 Úroveň vybavení informačními technologiemi

Zdroj: Vlastní

Z 37 respondentů je 30 (81,1 %) spokojeno se současným stavem informačních technologií. 13,5 % projevilo nespokojenost se současným stavem a 5,4 % neoznačilo žádnou z nabízených možností. Pro společnost je směrodatné, zda nespokojenost respondentů s nynějším vybavením je relevantní.

Úroveň podnikového informačního systému

Tvrzení č. 14 (Je dle Vašeho názoru informační podnikový systém na adekvátní úrovni - získávání, zpracování a dostupnost dat a informací) uvádí na základě zpracovaných odpovědí spokojenost či nespokojenost s podnikovým informačním systémem. Data jsou uvedena v grafu č. 4-14.



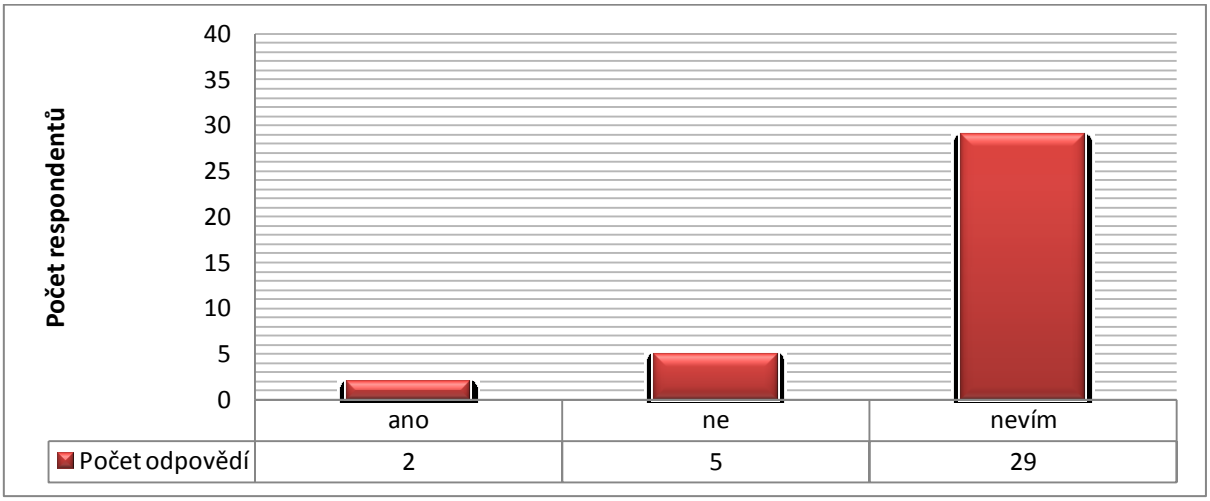
Graf 4-14 Úroveň podnikového informačního systému

Zdroj: Vlastní

83, 8 % respondentů je spokojeno se současným stavem informačního systému. 5,4 % shledává určité nedostatky či mezery v dané oblasti a 8,1 % dotazovaných označilo možnost *nevím*. 2,7 % pak neoznačilo žádnou z nabízených možností.

Podnikový dokument vztahující se k informační bezpečnosti

Úkolem tvrzení č. 15 (Existuje nějaký podnikový dokument zabývající se informační bezpečností) je zjistit, zda v podniku existuje dokument zabývající se právě informační bezpečností. Jednotlivé odpovědi jsou ke zhlédnutí v následujícím grafu č. 4-15.



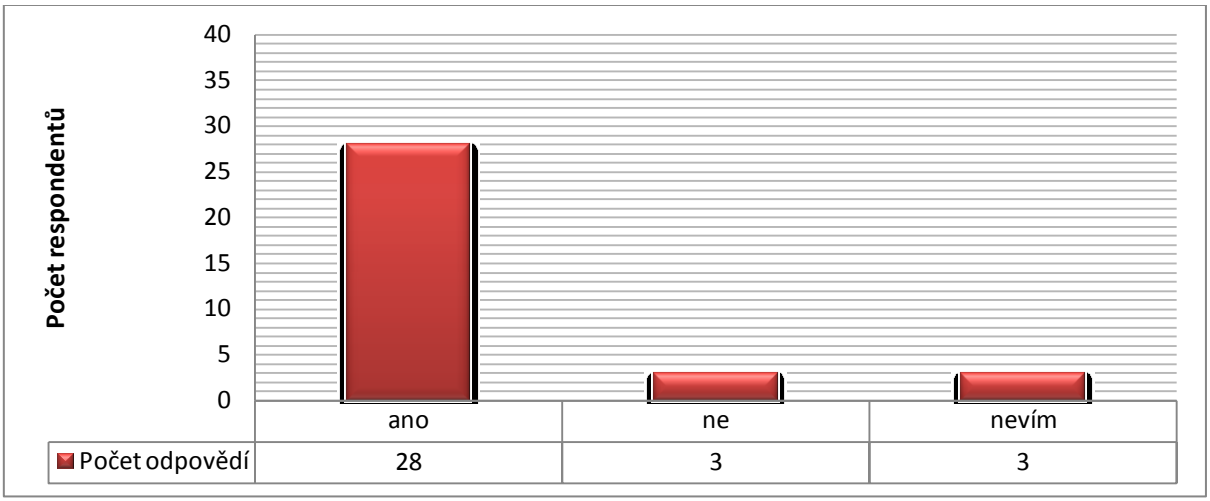
Graf 4-15 Existence podnikového dokumentu o informační bezpečnosti

Zdroj: Vlastní

Odpověď s nejčastějším výskytem byla možnost *nevím*, a to více než 78 % z celkového počtu respondentů, což může být znakem toho, že dokument existuje, ale není využíván, nebo jeho zpracování chybí úplně. 13,5 % označilo možnost *ne* a pouze 5,4% odpověď *ano*. 2,7 % pak neoznačilo žádnou z nabízených možností. Z průzkumu tedy vyplývá, že podniku chybí transparentní a plošný dokument pro všechny úrovně řízení.

Vytvoření interního dokument v oblasti informační bezpečnosti

Tvrzení č. 16 (Měl by být takový dokument vytvořen – návod, jak se zachovat v případě informačních problémů, koho oslovit, jak reagovat, atd.) přímo navazuje na předchozí, pakliže respondenti odpověděli *ne* či *nevím*. Vztahuje se tak na postoj k vytvoření příslušného dokumentu zabývajícího se informační bezpečností. Výsledná zjištění jsou uvedena v grafu č. 4-16.



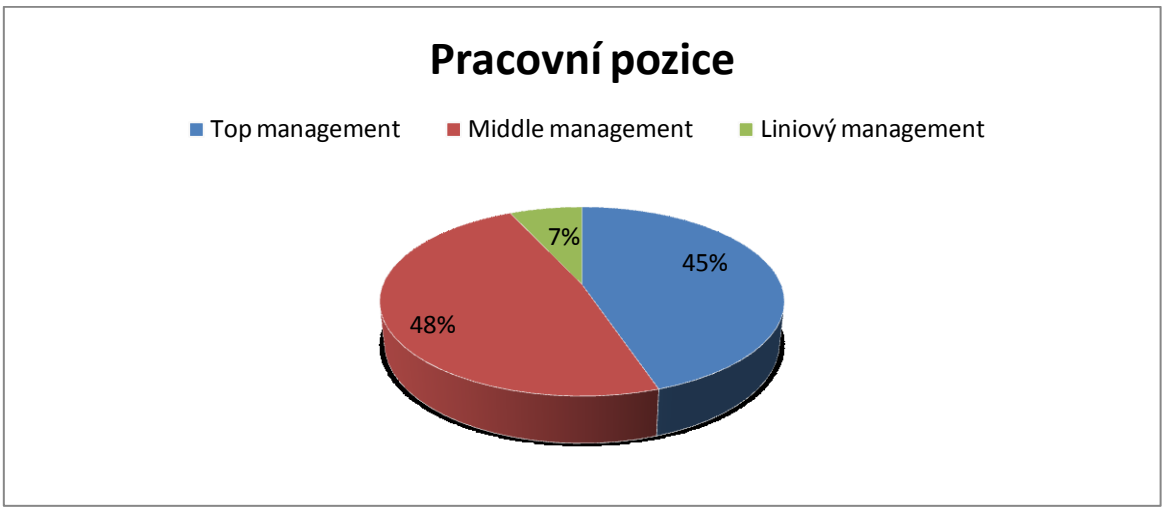
Graf 4-16 Vytvoření dokumentu o informační bezpečnosti

Zdroj: Vlastní

80 % respondentů je pro vytvoření interního dokumentu zabývajícího se informační bezpečností. Odpovědi *ne* a *nevím* označilo shodně 8,6 % dotazovaných. 2,9 % pak nezvolilo žádnou z nabízených možností. Ze zpracovaných dat vyplývá, že pro většinu respondentů je vypracování určitého „návodu“, jak postupovat v krizových situacích, důležité.

Pracovní pozice respondentů

Posledním dotazem uzavírající celý dotazník bylo zjištění pracovní pozice v podniku. Odpovědi byly roztřízeny do jednotlivých stupňů managementu – top management, middle management a liniový management. Výsledky jsou prezentovány v níže uvedeném grafu č. 4-17.



Graf 4-17 Pracovní pozici respondentů

Zdroj: Vlastní

Největší zastoupení respondentů je v top a middle managementu, menší část je potom v managementu liniovém. 5 % dotazovaných nevyplnilo svou pracovní pozici, což mohlo být zapříčiněno nedůvěrou v anonymní zpracování výsledků, jelikož každý dotazník byl odeslán z osobní emailové adresy, čímž bylo pochopitelně k dispozici i celé jméno respondenta. Výsledky ale byly vyhodnoceny tak, aby anonymita byla zachována, tzn. zařazení do obecné kategorie v rámci podnikové pracovní hierarchie. Vzhledem k povaze dotazníku jsou výsledky pouze informativního charakteru, jelikož výběr respondentů byl čistě náhodný, jedinou podmínkou byl přístup a využití počítače.

4.4. Shrnutí získaných poznatků

K tomu, abychom získali potřebná data k analýze současné situace podniku v rámci bezpečnosti informací, jsme použili metodu dotazníkového šetření, která nám následně umožnila vyhodnotit aktuální stav.

Významnost informací a jejich bezpečnost je pro respondenty vnímána jako důležitá součást podnikové kultury. Na druhou stranu jsou alarmujícím nedostatkem chybějící školení v dané oblasti, které mohou předejít případnému ohrožení celého podniku. 60 % respondentů se setkalo s bezpečnostním incidentem a jako nejčastěji byly uváděny spam a počítačový virus. V případě teoretických či praktických znalostí byly odpovědi s největším výskytem Trojský kůň, spam a počítačový virus.

V oblasti bezpečnosti a podpory informačního systému a ochrany dat a informací respondenti odpovídali ve dvou odlišných dimenzích. První je pozitivního charakteru, kdy jsou přesvědčeni o adekvátním přístupu ze strany podniku. Druhá varianta charakterizuje nevědomost či nejistotu dotazovaných o dané problematice.

V rámci všech respondentů má 95 % volný přístup k internetu, což pro firmu může znamenat potenciální vnější hrozbu, pakliže jeho uživatelé nejsou dostatečně obeznámeni s riziky. Vnímaný aspekt důležitosti bezpečného používání internetu je v podniku na vysoké úrovni, což platí také pro neposkytnutí informací osobě mimo podnik.

Odpovědnost za bezpečnost dat a informací je ve společnosti poněkud sporná. Zhruba polovina respondentů považuje za kompetentní pouze IT oddělení a druhá polovina jak IT, tak i management. Z toho můžeme usoudit, že odpovědnost není jednoznačně stanovena. Při řešení závažného problému v dané oblasti by se pak 68 % obrátilo na IT oddělení a 30 % jak na IT, tak i na svého nadřízeného. V této sféře je přístup podniku poněkud nesourodý a měl by být ustanoven jednoznačný a transparentní postup a odpovědnost.

Firma disponuje kvalitními informačními technologiemi a informačním systémem. Jediným větším nedostatkem je neexistence interního dokumentu o informační bezpečnosti nebo jeho nedostatečná propagace.

Původní znění hypotéz bylo následující:

H1: *„Zaměstnanci nedisponují dostatečnými informacemi o potencionálních informačních hrozbách a jejich předcházení.“*

H2: *„Informační bezpečnost je výhradně v kompetencích IT oddělení.“*

H3: *„V podniku chybí zpracovaný dokument zabývající se informační bezpečností.“*

Hypotéza H1 byla částečně potvrzena. Někteří respondenti mají přehled o eventuálních hrozbách a rizicích, zhruba 40 % z nich odpovědělo, že se nikdy nesetkali s žádným bezpečnostním incidentem, což je prakticky nemožné. Hypotéza H2 byla opět částečně potvrzena, jelikož vznikla určitá nesourodost v odpovědích, kdy polovina z nich byla IT oddělení a druhá IT oddělení a management. Hypotéza H3 byla opět jen částečně potvrzena, neboť nebylo prokázáno, že dokument neexistuje. 78 % dotazovaných zvolilo možnost *nevím*.

Z širšího pohledu má firma velmi dobré zázemí, podstatné je pouze detailně propracovat určité nedostatky jako přesné stanovení odpovědnosti, kompetencí, základní školení o informačních hrozbách a zpracování interního dokumentu zabývající se informační bezpečností.

5 DOPORUČENÍ PRO MANAGEMENT ORGANIZACE

Ve vztahu na příslušná zjištění v dotazníkovém šetření bylo vytvořeno několik stěžejních doporučení pro vedení podniku. V závislosti na potenciálních nákladech a časových dispozicích vzniklo několik variant jednotlivých řešení.

5.1. Školení

Firma by měla zvážit možnost školení svých zaměstnanců a to na všech úrovních organizační struktury. Přispělo by k všeobecnému rozšíření povědomí o důležitosti podnikových dat a informací, o potenciálních hrozbách, jejich případnému řešení, bezpečnému používání internetu, neposkytnutí citlivých informací a dat externímu subjektu a celkovému prohloubení znalostí v dané oblasti.

Školení lze provádět klasickou cestou nebo také e-Learningovými programy. Firma pak musí posoudit, která volba je pro jejich potřeby výhodnější a efektivnější. Popřípadě lze uplatnit také kombinace těchto dvou metod. Například klasické školení pro běžné uživatele a e-Learningový kurz pro administrátory nebo manažery.

Basic training (prioritní) s pokrytím všech zaměstnanců, které by probíhalo jako jednorázové interní školení kompetentní osobou. Jednoduchá struktura a obsah by měly být zárukou úspěšného pochopení dané problematiky, která by zahrnovala vysvětlení významu informací, současných hrozeb, minimalizace rizik a jejich řešení aj. Základní celopodnikový program školení by měl být poté obnovován dle zvážení managementu, například pokud se objeví nové internetové či další hrozby. Společnost má možnost využít i školení externího, což je pak otázkou nákladů a možnosti školení interního, jeho kvality a časových dispozic kompetentních osob.

Upper training by byl určený pro vedením vymezenou skupinu, která potřebuje širší základnu znalostní v dané problematice. Jednalo by se s největší pravděpodobností o manažery, administrátory a další osoby zodpovědné za zabezpečení správných informací pro rozhodování a jejich následné zabezpečení. Existují externí řešení, která může firma využít.

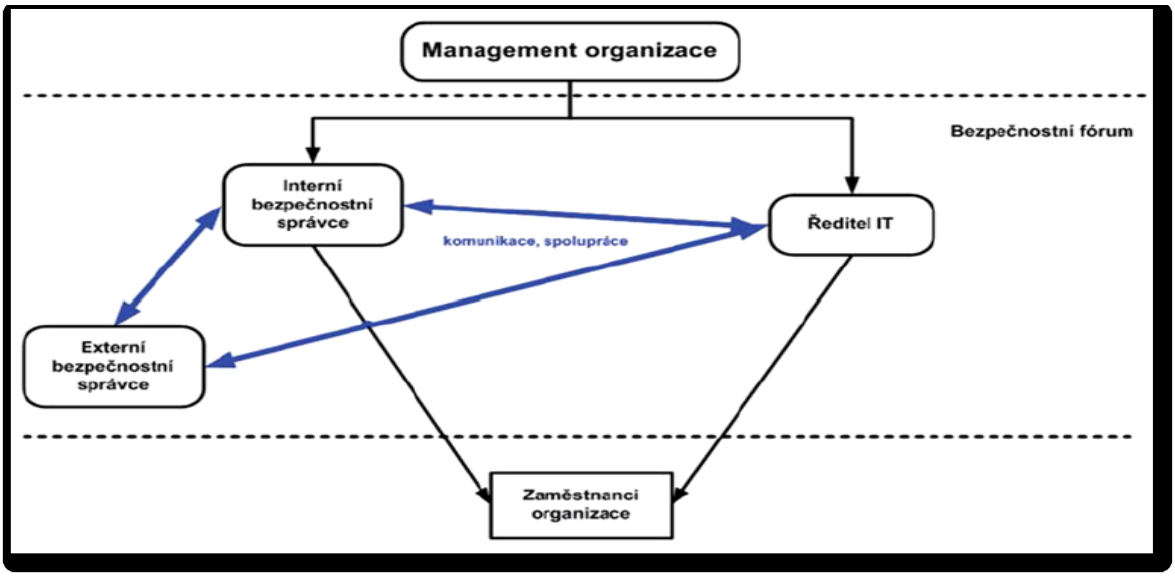
5.2. Správa bezpečnosti

V podniku by měla začít figurovat kompetentní osoba, která by zastávala roli bezpečnostního správce. Ten musí disponovat odpovídajícími znalostmi, musí mít povědomí o platné legislativě, normách a metodikách souvisejících s řízením bezpečnosti a jejím zajištěním. Kvalitní bezpečnostní správce se musí neustále vzdělávat, sledovat aktuální trendy a hrozby. Musí být v neustálém kontaktu nejen s oborem bezpečnosti, ale také s dalšími oblastmi informačních a komunikačních technologiích.

Rozhodující pro podnik je, zda tuto funkci zastoupí osoba z vnitřního prostředí nebo využije externí outsourcing. V obou případech musí zvážit pro a kontra, což obnáší například náklady na zaškolení, výběrová řízení, finanční odměnu, znalosti a zkušenosti potenciálního správce atd. Do základních funkcí bezpečnostního správce můžeme zahrnout:

- analýza a zpracování bezpečnostních incidentů
- analýza logů a dalších auditních záznamů
- údržba bezpečnostní dokumentace
- bezpečnostní školení zaměstnanců
- technické prověrky IS (testování)
- prověrky dodržování bezpečnostních pravidel
- reportování a souhrnné zprávy pro management

Dle níže zobrazeného schématu by mohl být zahrnut do organizační struktury externí bezpečnostní správce následujícím způsobem.



Obrázek 5-1 Začlenění externího správce do organizační struktury

Zdroj: Outsourcing správy bezpečnosti, 2009

5.3. Interní dokument

Prvním krokem k vytvoření informační strategie jsou nejrůznější analýzy, hodnocení, trendy a další klíčová kritéria. Následuje stanovení cílového stavu, který je složen ze dvou částí, a to globální architektura a její dílčí rozpracování, kam můžeme zařadit funkční a procesní architekturu, datovou architekturu, technologickou, softwarovou a hardwarovou architekturu, organizační a legislativní hlediska, personální hlediska, sociální a etická hlediska (Voznička, 2007).

Zároveň by mělo dojít k vyjasnění pravomocí a kompetencí mezi managementem a IT oddělením s dopadem na zaměstnance, kteří by se měli poté lépe orientovat v krizových situacích a rychlejšími reakcemi tak minimalizovat potenciální hrozby.

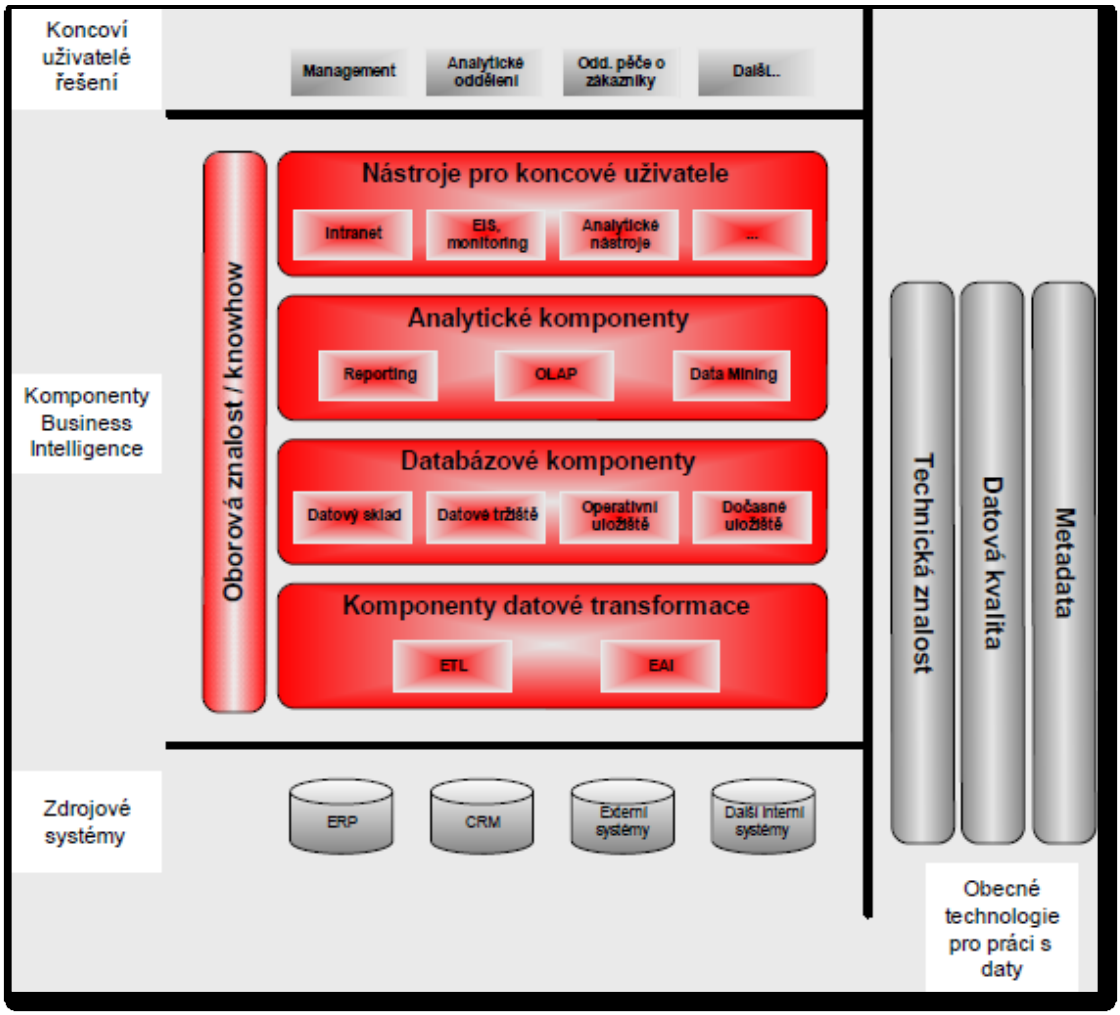
Vzhledem k časovým, finančním a kvalitativním kriteriím by podnik měl využít možnost externí spolupráce alespoň v první fázi tvorby informační strategie. Další vývoj již musí projednat vedení podniku.

5.4. Kvalitní zdroje informací

Hlavním kritériem při rozhodování se o velkých projektech a investicích jsou kvalitní data a informace, které podniku otevírají cestu ke zvýšení konkurenceschopnosti. Firma by tak měla mít vytvořenou strategii, jež stanovuje cestu k přístupu k potřebným informacím, a tím zároveň snižuje rozhodování za rizika či nejistoty.

Rozsáhlá oblast *Business Intelligence* se skládá z řady samostatných komponent, má vlastní architekturu i metodiky a s provozními systémy je provázaná řadou vazeb. Kromě tradičních aplikací, rozvíjí koncept MIS také EIS (Executive Information Systems) a nástroje dolování dat. Infrastruktura celé oblasti bývá založena na konceptu datového skladu. Existence datového skladu je předpokladem pro fungování nástrojů BI. Jedná se o ucelenou databázi optimalizovanou pro dotazování a analýzu dat, společně s nástroji, které dotazy, analýzy a kvalitní prezentaci výstupů umožňují. V datovém skladu jsou data integrována a ukládána, ať už se jedná o data z interních nebo externích zdrojů. Konečným cílem je poskytnout čitelné, organizované, analyzovatelné a v reálném čase dostupné informace z maxima podnikových databází i externích zdrojů, které jsou ve velkém rozsahu využitelné při řízení firmy či instituce (Tvrdíková, 2004).

Níže uvedený obrázek popisuje základní vrstvy při zavádění *Business Intelligence* do podnikové struktury. V případě analyzované společnosti by se jednalo o vytvoření právě čtyř uvedených úrovní, které by vycházely z dobře fungující informační základny a technologií, jako je systém MSD Navision.



Obrázek 5-2 Vrstvy řešení Business Intelligence

Zdroj: Business Intelligence, Datakon (2004)

Microsoft nabízí tzv. *Business Intelligence*, což jsou systémy poskytující komplexní a relevantní informace, které jsou získávány z dat generovaných nejrůznějšími provozními a informačními systémy. Pomocí *Business Intelligence* systémů může podnik integrovat a zpracovávat data ze všech možných datových zdrojů, ať už se jedná o databáze provozních aplikací, strukturovaná i nestrukturovaná textová data, Excel tabulky apod. Tyto systémy tedy poskytují relevantní a okamžité informace o fungování firmy, předdefinované reporty, možnost získávat rychle a pohodlně ad-hoc reporty, a v neposlední řadě umožňují publikovat informace pro strategické, ale i operativní rozhodování do nejrůznějších intranetových či extranetových serverů. Pokročilejší aplikace pak umožní vyhledávat v datech souvztažnost, vedoucí například k úsporám nákladů, efektivnějším marketingovým aktivitám, kvalitnější segmentaci vlastních zákazníků apod.

(Business Intelligence, 2012). Hlavní přínosy můžeme pak rozlišit do třech sfér – obchodní, finanční a IT oddělení.

IT ředitel

- spolehlivé řešení z pohledu serverové infrastruktury, jednodušší správa a zabezpečení
- rozšiřuje IT prostředí, nezavádí nové produkty
- úspora nákladů
- IT poskytuje komplexní řešení pro celou společnost
- využití běžných uživatelských prostředí, které uživatel zná a nemusí se je učit – nedělá chyby, příjemné řešení

Obchodní ředitel

- sledování výkonnosti obchodního týmu, řezy přes další dimenze (čas, region, obchodní/produktová skupina aj.)
- analýza chování zákazníku a efektivity obchodních a marketingových aktivit
- zjednodušení, zkvalitnění a zrychlení procesu reportingu
- k dispozici podklady pro zlepšení obchodních výsledků, k dispozici historická data

Finanční ředitel

- přehled o všech klíčových ukazatelích, o stavu financí firmy, nákladech atd.
- zjednodušení, zkvalitnění a zrychlení procesu reportingu
- K dispozici historie dat, nezávislé na změnách informačních systémů
- sdílení relevantních informací (čísel) relevantním lidem v relevantním čase

5.5. Náklady na financování vybraných řešení

Vzhledem ke komplexnosti informační strategie a individuálnímu přístupu ke každému subjektu je poměrně složité stanovit přesné náklady na navržená řešení. Vše se odvíjí od potřeb daného podniku a od výchozího stavu. Veškeré uvedené hodnoty jsou tak pouze orientační a pro přesné stanovení nákladů je vyžadována analýza a konzultace s vedením organizace.

V případě externího **vzdělávání** se rozlišuje, zda budou uživatelé školeni klasickou cestou, nebo prostřednictvím e-Learningu. V rámci klasického školení se zpravidla vytváří více tematických školení – např. specializované školení pro manažery, pro administrátory a pro běžné uživatele. V jednotlivých skupinkách pak probíhá osobní školení školiteli. Cena závisí na počtu vytvářených školeních (jejich obsahu a témat), potřebné míře detailu a samotném počtu školení. Oproti tomu e-Learningové školení je dodáváno formou univerzální aplikace, kterou je možné začlenit do stávající struktury (na intranet, do již existujících e-Learningů). Obsah se rovněž může tematicky dělit, míra detailu je závislá na bezpečnostním povědomí uživatelů. Cena se pohybuje v rozmezí 85 000 – 220 000 Kč.

Správa bezpečnosti a cena v případě externího řešení se outsourcing odvíjí od rozsahu dodávaných prací, což může zahrnovat jakoukoliv poskytovanou službu v oblasti bezpečnosti nebo jen konzultace v dané oblasti.

Tvorba **informační strategie** a její orientační částka je od 50 000 - do 100 000 Kč. Jedná se náklady související s konzultacemi, vypracováním návrhu strategie, obhajoby a konečné formulace. Součástí je i stanovení metrik pro vyhodnocení strategie v následujících letech a stanovení metodiky pro její udržování a rozvoj.

Business Intelligence je aplikace, která umožňuje sledovat, zpracovávat a vyhledávat jakákoliv data rychleji, efektivněji a poskytuje tak konkurenční výhodu při vyhodnocování informací. Odhad nákladů na integraci do podnikové kultury se ale paralelně odvíjí od potřeb podniku a výběru a hloubky jednotlivých řešení, která jsou dále specifikována pro každou jednotlivou společnost individuálně.

6 ZÁVĚR

Diplomová práce je rozčleněna na část teoretickou, v níž jsou ukotveny hlavní směry současných změn ve společnosti, základní pojmy a další důležitá východiska. Na ni navazuje část praktická s představením společnosti a dalším bodem je poté již samotná analýza současného stavu informační strategie. Posledním důležitým momentem jsou náměty pro management, které slouží jako podklady k dalšímu možnému vývoji informační strategie podniku.

První část práce s názvem teoretická východiska se zaměřuje na několik stěžejních oblastí dané problematiky. Zabývá se změnami ve společnosti – informatizace, vznik nových forem komunikace jako sociální sítě a jejich využití například v marketingových kampaních. Tyto změny se poté odráží i do podniků, které se musejí adaptovat a rozšiřovat o nové technologie a přístupy. Nová éra sebou přináší jak pozitivní, ale tak i negativní aspekty, kterými se práce zaobírá v několika odstavcích. Následující hlavní body jsou zaměřeny na informační hrozby, kybernetickou kriminalitu a jednotlivé konkrétní případy nebezpečí jak pro firmy, tak i běžné uživatele jako je phishing, pharming nebo malware. V neposlední řadě je v diplomové práci zmíněn také současný stav v České republice a zásadní nedostatky. Podstatným bodem je zvládání informačních hrozeb v podniku, které je podmíněno kvalitní informační strategií.

Dalším bodem byl popis analyzované společnosti LUKROM, spol. s r.o., který zobrazuje její historii, organizační strukturu a současný vývoj podniku. Podnik funguje v rámci holdingového uskupení, jenž disponuje necelými 300 zaměstnanci. Informační strategie by měla být důležitým prvkem v podnikové kultuře, aby rizika spojená se ztrátou dat a informací byla stlačena na co nejnižší úroveň.

Část analytická je tvořena z několika fází – tvorba dotazníku, stanovení počtu respondentů, určení hypotéz, pilotáž a následný samotný průzkum. Metoda dotazníkového šetření byla uskutečněna pomocí emailové komunikace. Hlavním cílem bylo zajištění podkladů k následné analýze současné situace podniku v oblasti informační bezpečnosti, kdy jednotlivé odpovědi jsou zpracovány v grafickém zobrazení, doplněné o komentáře pomocí jednoduché statistiky a subjektivní názory a připomínky autorky práce. Očekávání ohledně výsledku průzkumu byla pouze částečné potvrzena a to u každé ze tří hypotéz.

Z širšího hlediska má společnost velmi dobré zázemí a podnikovou kulturu, což jsou jednoznačné konkurenční výhody. Pakliže integruje informační strategii, její konkurenceschopnost se bude jen zvyšovat. Komplexnost této strategie pro LUKROM, spol. s r.o., znamená zaměření se pouze na oblasti, v nichž byly prokázány určité mezery a nedostatky. Tzn. například školení zaměstnanců, postupy při bezpečnostním incidentu, posílení této problematiky na manažerské úrovni apod. Kapitola je pak uzavřena doporučeními pro management, která představují reálná řešení, z nichž je možné si vybrat na základě potřeb organizace a dle uvážení nákladů na realizaci navrženého řešení. Financování těchto rozhodnutí je poněkud nákladnější, ale z dlouhodobého hlediska může taková investice posunout podnik o několik úrovní výš než jejich konkurenci a to v rámci získávání a zpracovávání informací, bezpečnosti a správy interních dat a informací, kvalitnější zázemí při rozhodování o velkých projektech atd.

Cílem diplomové práce bylo nastínit současnou situaci v podniku LUKROM, spol. s r.o., v oblasti informační strategie, posouzení nedostatků a předností pomocí dotazníkového šetření a návrh praktických řešení s hrubým odhadem nákladů. Téma informační bezpečnosti je důležitým bodem k diskuzi pro vedení každého podniku, jelikož důsledky při podceňování očividných hrozeb, které se již zdaleka netýkají jen běžných uživatelů či phishingových útoků na banky, mohou být fatální. Ztráta interních dat a informací, podnikového know-how či vniknutí a zablokování systému je v současné době tím jednodušší, čím víc organizace bude popírat, že ochrana a předcházení těchto rizik se skutečně vyplatí.

SEZNAM POUŽITÉ LITERATURY

Knihy

BASL, J., BLAŽÍČEK, R. *Podnikové informační systémy.* Praha: Grada Publishing, 2008. ISBN: 978-80-247-2279-5.

JIROVSKÝ, Václav. *Kybernetická kriminalita.* Praha: Grada, 2007. ISBN 80-247-1561-9.

GALLIERS, D. R., LEIDNER, E. D. *Strategic information management.* Velká Británie: British Library, 2003. ISBN: 0-7506-5619-0.

KEŘKOVSKÝ, M., DRDLA, M. *Strategické řízení firemních informací. Teorie pro praxi.* Praha: C. H. Beck, 2003. ISBN 80-7179-730-8.

KEŘKOVSKÝ, M., VYKYPĚL, O. *Strategické řízení. Teorie pro praxi.* Praha: C. H. Beck, 2006. ISBN: 80-7179-453-8.

KRCMAR, Helmut. *Informationsmanagement.* Berlin: Springer Berlin Heidelberg, 2005. ISBN: 3-540-23015-7.

TVRDÍKOVÁ, Milena. *Aplikace moderních informačních technologií v řízení firmy.* Praha: Grada Publishing, 2008. ISBN: 978-80-247-2728-8.

VRANA, I., RICHTA, K. *Zásady a postupy zavádění podnikových informačních systémů.* Praha: Grada Publishing, 2005. ISBN: 80-247-1103-6.

VYMĚTAL, J., A. DIAČIKOVÁ a M. VÁCHOVÁ. *Informační a znalostní management v praxi.* Praha: LexisNexis CZ, 2006. ISBN 80-86920-01-1.

Diplomová práce

OHLIGER, A. Erhöhung der Markttransparenz und Verbesserung der Verbraucherinformation durch Lebensmittelkennzeichnungen: Eine Analyse des Fischetikettierungsgesetzes aus informationsökonomischer Sicht. Norderstedt, 2005. Diplomová práce. Institut für Agrarpolitik, Marktforschung und Wirtschaftssoziologie.

Internetové zdroje

ADAPTIC. *E-learning*. © Redakční systém Colibri CMS, 2005–2012 [online]. [cit. 2012-06-26]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/e-learning/

BEDNÁŘ, Vojtěch. LUPA. CZ In: *Pharming je zpět a silnější.* [online]. March 23, 2007, 6:25 am [cit. 2012-05-02]. Dostupné z: http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/

BEZPEČNÝ INTERNET. CZ. *Phishing a pharming.* [online]. [cit. 2012-03-28]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

BRECHLEROVÁ, Dagmar. SYSTEM ONLINE In: *Řešení informační bezpečnosti.* [online] [cit. 2012-03-25]. Dostupné z: http://www.systemonline.cz/clanky/reseni-informacni-bezpecnosti-1-cast.htm

CIO. *Malé a střední podniky podceňují hrozbu cílených kyberútoků.* [online]. [cit. 2012-04-15]. Dostupné z: http://businessworld.cz/aktuality/male-a-stredni-firmy-podcenuji-hrozbu-cilenych-kyberutoku-8218

CFOWORLD. *Počítačová gramotnost v Česku, aneb vítejte v Zimbabwe*. [online]. [cit. 2012-06-26]. Dostupné z: http://cfoworld.cz/trendy/pocitacova-gramotnost-v-cesku-aneb-vitejte-v-zimbabwe-892

CLOUD. CZ. *Objem dat na světě se každé dva roky více než zdvojnásobí.* [online]. [cit. 2012-02-10]. Dostupné z:http://www.cloud.cz/tiskove-zpravy/176-objem-dat-na-svt-se-kade-dva-roky-vice-ne-zdvojnasobi.html

COMPUTERWORLD. CH. *Informationsstrategie in fünf Schritten.* [online]. © 1996 - 2012 [cit. 2012-04-10]. Dostupné z: http://www.computerworld.ch/whitepapers/it-management/artikel/informationsstrategie-in-fuenf-schritten-56490

CSIRT. CZ. *Incident handling statistics.* [online]. © 2011 [cit. 2012-03-21]. Dostupné z: http://www.csirt.cz/files/csirt/statistics/stats.html

ČESKÝ STATISTICKÝ ÚŘAD. *Uživatelé Facebooku – mezinárodní srovnání.* [online]. © Český statistický úřad, 2012 [cit. 2012-01-15]. Dostupné z: http://www.czso.cz/csu/katalog.nsf/hledat?SearchView&count=20&searchmax=10000&se

archorder=1&searchfuzzy=1&query=%28%28facebook%29%29&database=all&kraje=all&skupiny=all&start=1

ČESKÝ STATISTICKÝ ÚŘAD. *Informační společnost v číslech 2011.* [online]. © Český statistický úřad, 2012 [cit. 2012-01-15]. Dostupné z: http://www.czso.cz/csu/2011edicniplan.nsf/p/9705-11

DATAKON. *Business Intelligence.* [online]. [cit. 2012-05-27]. Dostupné z: http://www.datakon.cz/datakon08/d04_tut_pour.pdf

DOČEKAL, Daniel. LUPA. CZ In: *Sociální sítě si podmanily svět (fakta a čísla hlavně o Evropě)* [online]. Sept 26, 2011, 6 am [cit. 2012-01-15]. Dostupné z: http://www.lupa.cz/clanky/socialni-site-si-podmanily-svet-fakta-a-cisla-hlavne-o-evrope /

DOČEKAL, Daniel. LUPA. CZ In: *Sociální sítě si podmanily svět (fakta a čísla hlavně o Evropě)*. [online]. Sept 26, 2011, 6:25 am [cit. 2012-01-26]. Dostupné z: http://www.lupa.cz/clanky/socialni-site-si-podmanily-svet-fakta-a-cisla-hlavne-o-evrope/

FONDY EVROPSKÉ UNIE. *Horizontální priority v projektové žádosti.* [online]. [cit. 2012-01-20]. Dostupné z: http://www.strukturalni-fondy.cz/Informace-o-fondech-EU/Rizeni-fondu-EU/Horizontalni-priority/Horizontalni-priority-2004-2006/Horizontalni-priority-v-projektove-zadosti

FONDY EVROPSKÉ UNIE. *Rozvoj informační společnosti ve veřejné správě.* [online]. [cit. 2012-01-20]. Dostupné z: http://www.strukturalni-fondy.cz/getdoc/99662404-33af-40e4-9765-4812d7b3d471/Rozvoj-informacni-spolecnosti-ve-verejne-sprave

GREGOR, Pavel. RESSELER MAGAZINE In: *ČR ztrácí v digitální vzdělanosti a informatizaci.* [online]. [cit. 2012-01-20]. © Reseller Magazine OnLine Web o businessu v informačních technologiích, 2009 – 2012 [cit. 2012-01-20]. Dostupné z: http://www.reselleronline.cz/cr-ztraci-v-digitalni-vzdelanosti-a-informatizaci

HOAX. CZ. *Phishing.* [online]. © 2000 - 2012 [cit. 2012-03-02]. Dostupné z: http://www.hoax.cz/phishing/ing---info-plus-s-elektronickymi-vypisy-11152011/

HOAX. CZ. *Hoax.* [online]. © 2000 - 2012 [cit. 2012-03-02]. Dostupné z: http://www.hoax.cz/hoax/http:/www.hoax.cz/hoax/

HOLEČEK, Bohumír. *Zpráva nezávislého auditora.* [online] [cit. 2012-04-17]. Dostupné z:

http://www.lukrom.cz/images/stories/web/Dokumenty/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1vy/VZ%202010.pdf

IBM. *Chytrá rozhodnutí vedoucí k optimalizaci výkonu*. [online]. [cit. 2012-02-24]. Dostupné z: http://www-05.ibm.com/cz/gbs/bcs/bcs_centeroptimization.html

IBM. *Eine effektive Informationsstrategie dank Business Analytics and Optimalization.* [online]. © 2010 [cit. 2012-03-25]. Dostupné z: ftp://public.dhe.ibm.com/software/ch/de/multimedia/pdf/transkript-ibm-business-analytics-optimization-de.pdf

IBM. *Business Analytics and Optimalization.* [online]. © 2010 [cit. 2012-03-25]. Dostupné z: http://www-935.ibm.com/services/ch/bcs/bao/index.html

IHNED. CZ. *Obama podepsal nová pravidla pro vedení kybernetických válek.* [online]. © 1996 - 2012 [cit. 2012-03-02]. Dostupné z: http://zpravy.ihned.cz/svet/c1-52146300-obama-podepsal-nova-pravidla-pro-vedeni-kybernetickych-valek

ITIL. *Bezpečnost IS/IT* [online]. © 2007 [cit. 2012-03-16]. Dostupné z: http://www.itil.cz/index.php?id=1003

IT SOLUTION. *Informační strategie.* [online]. [cit. 2012-03-21]. Dostupné z: http://www.itsolution.cz/informacni-strategie.a11.html

JIROVSKÝ, V., V. HNÍK a O. KRULÍK. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY In: *Kybernetické hrozby: Výzva pro moderní společnost.* [online]. [cit. 2012-02-29]. Dostupné z: http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/kyberneticke_hrozby.pdf

KRČMA, Pavel. LIDOVKY. CZ In: *Kyberválka není výmysl, tvrdí vývojář antivirů.* [online]. Nov 14, 2011, 8:02 pm [cit. 2012-02-29]. Dostupné z: http://byznys.lidovky.cz/kybervalka-neni-vymysl-tvrdi-vyvojar-antiviru-frx-/firmy-trhy.asp?c=A111113_095835_ln_domov_spa

LUKROM. *Profil.* [online]. © 2012 [cit. 2012-04-10]. Dostupné z: http://www.lukrom.cz/cs/predstaveni-spolecnosti.html

MICROSOFT. *Business Intelligence.* [online]. © 2012 [cit. 2012-04-23]. Dostupné z: http://www.microsoft.com/cze/reseni/stredni-a-velke-spolecnosti/business-intelligence.aspx

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Bezpečnost a prevence.* [online]. © 2010 [cit. 2012-02-29]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mw%3D%3D

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Standardy a doporučení.* [online]. © 2010 [cit. 2012-02-26]. Dostupné z: http://aplikace.mvcr.cz/archiv2008/micr/files/2705/06_nsib_cr_priloha_2_v0_8__2_.pdf

MODERNÍ ŘÍZENÍ. *Informační exploze a exformace.* [online]. © 1996-2011 [cit. 2012-01-26]. Dostupné z: http://modernirizeni.ihned.cz/1-10065470-20886120-600000_detail-40

MUSTACA,Sorin. AVIRA In: *How does a phishing website gets access to our account number* [online]. Mai 15, 2012, 6:15 am [cit. 2012-05-02]. Dostupné z: http://techblog.avira.com/2012/05/15/security-101-april-questions-answers/en/

NOVINKY. CZ. *Nad světem visí hrozba kyberválky, varuje expert.* [online]. © 2012 [cit. 2012-01-28]. Dostupné z: http://www.novinky.cz/internet-a-pc/249607-nad-svetem-visi-hrozba-kybervalky-varuje-expert.html?ref=zpravy-dne

NOVINKY. CZ. *Počítačovým hrozbám kralují viry šířící se přes USB flash disky.* [online]. © 2003 - 2012 [cit. 2012-03-15]. Dostupné z: http://www.novinky.cz/internet-a-pc/bezpecnost/255356-pocitacovym-hrozbam-kraluji-viry-sirici-se-pres-usb-flash-disky.html?ref=ostatni-clanky

PCWORLD. *Co je sociální inženýrství? – 1. díl.* [online]. Juni 02, 2012 [cit. 2012-06-26]. Dostupné z: http://pcworld.cz/internet/co-je-socialni-inzenyrstvi-1-dil-44361

PINKAVA, Jaroslav. ROOT.CZ In: *Bezpečnostní střípky: Počítačová kriminality je největší světovou kriminální hrozbou.* [online]. Sept 27, 2010, 0 am [cit. 2012-01-26]. Dostupné z: http://www.root.cz/clanky/bezpecnostni-stripky-pocitacova-kriminalita-je-nejvetsi-svetovou-kriminalni-hrozbou/

SAK, P., SAKOVÁ, K. LUPA. CZ In: *Počítačová gramotnost a způsoby jejího získávání*. [online]. Sept 26, 2011, 6:30 am [cit. 2012-06-26]. Dostupné z: http://www.lupa.cz/clanky/pocitacova-gramotnost-zpusoby-ziskavani/

SLINTÁK, Jiří. SVĚT SÍTÍ In: *Nebezpečí sociálního inženýrství a jak se mu účinně bránit.* [online]. © Svět sítí & Infinity a. s., 2000 – 2012, Oct 26, 2009 [cit. 2012-06-26]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Nebezpeci-socialniho-inzenyrstvi-a-jak-se-mu-ucinne-branit-26102009

SOBOL, Tomáš In: *Informační společnost.* [online]. [cit. 2012-01-20]. Dostupné z: http://www.sfiles.host.sk/work/inf_spol.html#up

TOMÁŠ, Marek. INFLOW In: *Informační problém v díle Alberta Gora Země na misce vah.* [online]. July 05, 2010, [cit. 2012-02-16]. Dostupné z: http://www.inflow.cz/node/2884/edit%3Fdestination%3Dadmin%252Fejournal%252Fedit%252F1%252F_%252F37

TVRDÍKOVÁ, M. *Nástroje Business Intelligence.* [online] [cit. 2012-05-28]. Dostupné z: http://cev.cemotel.cz/programovani_a_tvorba_sw_1975-2004/2004/304.pdf

VOŘÍŠEK, J., NOVOTNÝ, O. In: *Digitální cesta k prosperitě – shrnutí hlavních zjištění a doporučení.* [online]. Sept 2006 [cit. 2012-01-15]. Dostupné z: http://www.reselleronline.cz/files/clanky_upld/digitalni_cesta_summary_20101003.pdf

WAIC, Vlastimil. STAHUJ. CZ In: *Malware napadl vloni 10 miliónů PC*. [online]. March 12, 2009 [cit. 2012-03-04]. Dostupné z: http://magazin.stahuj.centrum.cz/malware-napadl-vloni-10-milionu-pc/

Interview

ŠPIDLA, Aleš. Interview. In: *Studio ČT24*. TV, ČT24, 15. března 2010.

SEZNAM POUŽITÝCH ZKRATEK

ICT	informační a komunikační technologie
HW	hardware
SW	software
ČSN	Česká státní norma
IT	informační technologie
IS	informační systémy

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

PROHLÁŠENÍ O VYUŽITÍ VÝSLEDKŮ DIPLOMOVÉ PRÁCE

Prohlašuji, že

- jsem byla seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou (bakalářskou) práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová (bakalářská) práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové (bakalářské) práce. Souhlasím s tím, že bibliografické údaje o diplomové (bakalářské) práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou (bakalářskou) práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne …… Bc. Lucie Odehnalová

Adresa trvalého pobytu studenta:
Polní 45 82, Zlín 760 05